Bayerischer Landtag
10. Wahlperiode

Drucksache **10/8252**
30. 10. 85

Der Landesbeauftragte für den Datenschutz
Nr. DSB/ 1 - 510 - 8

München, den 30. Oktober 1985

An den
Herrn Präsidenten
des Bayerischen Landtags
München

Betreff: **Siebter Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz**

Sehr geehrter Herr Landtagspräsident!

In der Anlage übersende ich gemäß Art. 28 Abs. 4 des Bayerischen Datenschutzgesetzes den siebten Tätigkeitsbericht.

Der Beirat hat den Entwurf in seiner Sitzung am 22. Oktober 1985 vorberaten.

Mit vorzüglicher Hochachtung

Dr. Konrad Stollreither

Siebter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum 1984/1985

Inhaltsübersicht

		Seite
1.	**Vorbemerkung**	4
2.	**„Ich habe nichts zu verbergen"**	4
3.	**Gesundheit**	5
3.1.	Krebsregistrierung	5
3.2.	Erstellen einer Patientenliste für die Polizei	5
3.3.	Aufbewahrung äztlicher Aufzeichnungen bei Auflösung einer Arztpraxis ohne Übertragung auf einen Nachfolger	6
3.4.	Erhebung von Personal-Gesundheitsdaten bei Dritten	7
3.5.	Datenerhebung über Ärzte und anderes Klinikpersonal	7
3.6.	Weitergabe von Arztbriefen an Sozialpsychiatrische Dienste	8
3.7.	Hinweis auf die Freiwilligkeit bei der Erhebung von Gesundheitsdaten	8
3.8.	Anfragen von Krankenhäusern bei Meldeämtern	8
3.9.	Fertigung von Fotografien bei der Patientenaufnahme in Bezirkskrankenhäusern	9
3.10.	Anforderung von Krankenunterlagen durch ein Versorgungsamt	9
3.11.	Schreibdienstuntersuchung in einem Krankenhaus	10
3.12.	Offenbarung von Patientendaten durch ein Krankenhaus gegenüber einer Sparkasse	10
3.13.	Erstellung einer Patientenstrukturanalyse durch eine Beratungsgesellschaft	10
3.14.	Nutzung von Ärzteanschriften für Wahlwerbung	10
4.	**Sozialbehörden**	11
4.1.	Suche nach Unterhaltspflichtigen – unter Verwendung eines problematischen Mittels	11
4.2.	Telefonische Auskunft über Sozialdaten – an den Falschen	11
4.3.	Übermittlung der Anschriften von Schulabgängern aus dem Melderegister an Krankenkassen	11
4.4	Vorlage und Abgabe von Sozialhilfeakten an staatliche Archive	12

4.5. Datenverarbeitung durch Unternehmen im Auftrage ihrer Betriebskrankenkassen . . . 12

4.6. Darf eine Gemeinde Rentendaten speichern? . . . 13

4.7. Auftragsdatenverarbeitung – auftragswidrige Datennutzung durch den Auftragnehmer 13

4.8. Umfang der Datenerhebung beim Antrag auf Sozialhilfe . . . 14

4.9. Sozialbericht Suchtkranke . . . 14

4.10. Geschützte Sozialdaten – auf Krankenscheinen ohne Schutz . . . 15

4.11. Datenerhebung aus Anlaß eines „mißglückten Arbeitsversuches" . . . 15

4.12. Schutz von Daten, die einem Arzt anvertraut wurden, der vom Sozialleistungsträger beschäftigt wird . . . 15

4.13. Welche medizinischen Daten darf eine Krankenkasse einem anderen Sozialleistungsträger offenbaren? . . . 16

4.14. Überprüfung von Datenerhebung und Speicherung durch die Landesstiftung „Hilfe für Mutter und Kind" . . . 17

4.15. Krankengeschichten in Sozialakten? . . . 17

5. Polizei . . . 18

5.1. Zur Lage des Datenschutzes . . . 18

5.2. Schwerpunkte meiner Tätigkeit . . . 18

5.3. Führung und Auswertung von Kriminalakten (Bürger von 3 bis 101 Jahre) . . . 18

5.3.1. Kriminalaktennachweis (KAN) . . . 19

5.3.2. Überprüfung der Kriminalaktensammlungen 21

5.3.3. Kriminalaktensammlung beim Polizeipräsidium München . . . 22

5.4. Neuordnung der polizeilichen Meldewege . 22

5.5. Personengebundene Hinweise . . . 24

5.6. Erkennungsdienstliche Behandlung . . . 24

5.7. Novellierung des Polizeirechts . . . 25

5.8. Polizeilicher Staatsschutz . . . 28

5.8.1. Führung der Vorgänge . . . 28

5.8.2. Informationsaustausch . . . 28

5.8.3. Errichtung einer Arbeitsdatei PIOS – Innere Sicherheit (APIS) . . . 29

6. Verfassungsschutz . . . 30

6.1. Prüftätigkeit beim Bayer. Landesamt für Verfassungsschutz . . . 30

6.2. Sicherheitsüberprüfungen und der Fall N. . 31

6.3. Bereichsspezifischer Datenschutz bei Nachrichtendiensten . . . 32

6.4. Auskunftsanspruch gegenüber Verfassungsschutzbehörden . . . 33

7. Justiz . . . 34

7.1. Überblick . . . 34

7.2. Mitteilungen in Zivilsachen . . . 34

7.3. Mitteilungen in Strafsachen . . . 36

7.4. Schuldnerverzeichnis . . . 36

7.5. Weitergabe gerichtlicher Entscheidungen . 38

7.6. Strafvollzug . . . 38

8. Städte und Gemeinden . . . 39

8.1. Nutzung von Daten Steuerpflichtiger für andere Zwecke der Gemeinde? . . . 39

8.2. Das Personalamt einer Stadt und die „Freiwilligen Wahlhelfer" . . . 39

8.3. Darf ein Erschließungs-Beitragspflichtiger von der Gemeinde erfahren, wieviel seine Nachbarn für Grundstücksverkäufe erhalten haben? . . . 40

8.4. Antrag auf Erteilung eines Führungszeugnisses mit falschen Angaben . . . 40

8.5. Nach dem Urlaub kommt die Polizei . . . 40

8.6. Fehlsubventionen im Wohnungswesen: . . . 41

8.7. Datenübermittlung Gemeinde – Amt für Landwirtschaft . . . 41

8.8. Datenerhebung für das „Zeugnis über das Nichtbestehen eines Vorkaufsrechts" . . . 41

8.9. Auskunft über Anschriften von Familien mit nichtschulpflichtigen Kindern und mit Hunden an die Bundesbahn . . . 42

8.10. Namensnennung in öffentlicher Gemeinderatssitzung? . . . 42

8.11. Nennung der Privatanschriften von Bauantragsstellern in öffentlicher Sitzung und in Protokollen des Bauausschusses . . . 42

8.12. Umgang mit Gewerbetreibenden-Daten . . 43

9. Einwohnermelderegister . . . 43

9.1. Wahlwerbung mit Meldedaten . . . 43

9.2. Veröffentlichung von Geburten, Eheschließungen und Sterbefällen . . . 43

9.3. Zum Verhältnis Hotelgast/Meldebehörde . . 44

9.4. Bayerische Meldedaten-Übermittlungsverordnung (BayMeldeDÜV) nach Art. 31 Abs. 5 MeldeG . . . 44

10. Steuerverwaltung . . . 46

10.1. Braucht das Finanzamt Krankheitsdiagnosen? . . . 46

10.2. Bekanntgabe von Steuerschulden durch Finanzämter in Pfändungsverfügungen . . . 46

10.3. Versand von Steuerbescheiden und Steuererklärungsvordrucken . . . 47

10.4. Welche Angaben auf Steuererhebungs-Formularen sind „Pflicht" – welche sind freiwillig? . . . 4

11. Personalwesen 47
11.1. Datenschutz bei Beihilfedaten 47
11.2. Zuordnung des betriebsärztlichen Dienstes einer Stadt zum Personalamt? 49
11.3. Telefongesprächsdatenerfassung 49
11.4. Darf die Personalstelle der Gemeinde Auskünfte über Mitarbeiter an deren Gläubiger oder an Kreditinstitute geben? 51
11.5. Mitteilung über nicht rechtswidrige Sterilisation oder nicht rechtswidrigen Abbruch der Schwangerschaft bei Arbeitsunfähigkeit von BAT-Angestellten 51
11.6. Weitergabe von Anschriften von Bewerbern für die Beamtenlaufbahn an Versicherungen 52
11.7. Personalsachbearbeiter oder Ausbildungsleiter als Vertrauensmann für eine Versicherung? 52
11.8. Weitergabe von Personaldaten zur Veröffentlichung durch Verbände 53

12. Statistik 53
12.1. Mikrozensus 1985 53
12.2. Volkszählung 53
12.3. Statistikdaten für Regionalplanung 54
12.4. Hochschulstatistik 54
12.5. Keine namentliche Befragung von Schülern mehr nach ihren Studien- und Berufswünschen 54

13. Schule und Hochschule 55
13.1. Persönlichkeitsschutz an Schulen 55
13.2. Datenerhebung für Forschungszwecke . . . 56
13.3. Datenerhebung für Zwecke der Schulverwaltung 56
13.4. Einsatz von Kleincomputern an der Schule . 57
13.5. Hochschuldaten (Hochschulstatistik) 57
13.6. Aushang von Klausurnoten 58

14. Archive 58
14.1. Notwendigkeit von Archivgesetzen 58
14.2. Bundesarchivgesetz-Entwurf 59
14.3. Bayerisches Archivgesetz – Sachstand . . . 60
14.4. Übergangslösung 60

5. Straßenverkehr 61
5.1. Führerschein auf Probe 61
5.2. Zentrales Verkehrs-Informationssystem (ZEVIS) 62

6. Weitere Probleme in der Verwaltung 62
6.1. Einhaltung des „Dienstweges" 62
6.2. Ergänzung der staatlichen Vordruckrichtlinien um Hinweise auf den Datenschutz . . . 62
6.3. Berücksichtigung des Datenschutzrechts im Vorbereitungsdienst der Rechtsreferendare 63

17. Neue Medien 63
17.1. Bildschirmtext 63
17.1.1. Zur Lage 63
17.1.2. Probleme der Umsetzung der Datenschutzregelung im Staatsvertrag durch die Deutsche Bundespost 64
17.1.3. Datenschutzfragen beim technischen System-Konzept der Deutschen Bundespost . 64
17.1.4. Datenschutzprobleme in der Praxis 65
17.1.5. Prüfungserkenntnisse 66
17.2. Medienerprobungs- und -entwicklungsgesetz (MEG) 67
17.2.1. Datenschutz-Regelungen 67
17.2.2. Abrechnung und wissenschaftliche Begleitforschung 67
17.3. Fernwirkdienste 68

18. Technischer und organisatorischer Bereich 69
18.1. Technische und organisatorische Grundsatzfragen 69
18.1.1. Anforderungen an die Protokollierung von Ablaufdaten für Revisionszwecke beim Einsatz von DV-Systemen mittlerer Größe . . . 69
18.1.2. Individuelle Datenverarbeitung 70
18.1.3. Elektronisches Büro 71
18.2. Kontrolle der technischen und organisatorischen Maßnahmen 71
18.3. Technische Einzelprobleme 72
18.3.1. Technische und organisatorische Maßnahmen zur Einhaltung des Persönlichkeitsschutzes 72
18.3.2. Vernichtung und Entsorgung von Datenträgern 73
18.3.3. Speicherkontrolle bei Online-Verfahren . . . 73
18.3.4. Die Chip-Karte 73
18.3.5. Fernwartung von DV-Systemen 74
18.3.6. Mikroverfilmung von Schriftgut 74
18.3.7. Kryptographie 75
18.4. Datensicherung bei den Neuen Medien . . . 76
18.4.1. Datensicherungsmaßnahmen bei Bildschirmtext 76
18.4.2. TEMEX, ein Daten-Dienst der Deutschen Bundespost 77

19. Datenschutzregister 77
19.1. Stand 77
19.2. Vollständigkeit des Datenschutzregisters und „Bagatell"-Dateien 78

20. Bankauskunftsverfahren 78

21. Datenschutz beim Bayerischen Rundfunk . 78

22. Weiterentwicklung des Datenschutzrechts 79

22.1. Umsetzung des informationellen Selbstbestimmungsrechts 79

22.2. Fortentwicklung von BDSG und BayDSG . . 80

22.2.1. Notwendigkeit ergänzender Regelungen . . 80

22.2.2. Anwendungsbereich des BDSG: 81

22.2.3. Zur Einführung von Zweckbindungsregelungen: 82

22.2.4. Zur Frage der Kontrollzuständigkeit des Bundes- bzw. Landesbeauftragten für den Datenschutz: 83

23. Der Beirat 84

24. Behandlung des sechsten Tätigkeitsberichts im Parlament 86

25. Arbeitsbedingungen der Geschäftsstelle . 87

26. Konferenz der Datenschutzbeauftragten . 87

Anhang Nr. 1 87

Anhang Nr. 2 88

Anhang Nr. 3 90

1. Vorbemerkung

Was Datenschutz ist und was er bewirkt, wird in der Öffentlichkeit immer weniger deutlich: Immer häufiger ist von „überzogenem Datenschutz" die Rede, nicht selten wird ein Fehlverhalten damit begründet, „der Datenschutz sei schuld", auch wenn Datenschutzfragen im betreffenden Fall gar nicht in Frage standen. Dies gilt nicht nur für den Sicherheitsbereich.

Über die Arbeit, die der Bayerische Landesbeauftragte für den Datenschutz und seine Mitarbeiter im Jahr 1984 – bis hinein ins Jahr 1985 – geleistet haben, erstatte ich im folgenden aufgrund von Art. 28 Abs. 4 des Bayerischen Datenschutzgesetzes dem Landtag und der Staatsregierung Bericht. Wie in den vergangenen Jahren weist er neben erfreulichen Verbesserungen auch Verstöße gegen datenschutzrechtliche Bestimmungen nach. Dies zeigt, daß die volle Wahrung der Persönlichkeitsrechte im Sinne des Grundgesetzes in der öffentlichen Verwaltung eine langfristige Aufgabe darstellt, deren Lösung wohl unvermeidbaren Schwankungen unterworfen ist. Bei Erfüllung dieser Aufgabe hat sich der „bayerische Weg", wie ich glaube, bewährt.

2. „Ich habe nichts zu verbergen"

... Ich habe nichts zu verbergen! So oder ähnlich lautet ein häufiger Einwand gegen die Notwendigkeit von Datenschutzmaßnahmen. Daß auch der harmlose Normalbürger in die Situation kommen kann, den Datenschutzbeauftragten massiv zum Einschreiten und Abstellen von Mißständen aufzufordern, zeigt folgender Fall, in dem ausgerechnet auch noch das „harmlose" Datum der Anschrift auslösender Faktor war: Eine Stadt hatte aus dem Melderegister auf eine Anfrage nach der Anschrift einer Frau, die mit Nachnamen und einem Vornamen bezeichnet war, Auskunft über die neue Anschrift einer Frau mit gleichen Nach- und Vornamen sowie einem weiteren Vornamen gegeben und hinzugefügt „ob Personengleichheit besteht, kann nicht festgestellt werden".

Der Frau deren („neue") Adresse bekanntgegeben worden war, widerfuhr daraufhin folgendes:

- Verschiedene Versicherungen forderten Versicherungsbeiträge (einmal mit Mahnbescheid).
- Eine Kfz-Zulassungsstelle erließ einen Bescheid über die zwangsweise Stillegung eines Pkw's.
- Eine Finanzamt forderte zur Abgabe der Umsatz- und Einkommenssteuererklärung auf.
- Die Allgemeine Ortskrankenkasse meldete eine Schadensersatzforderung an.
- Der Gerichtsvollzieher erschien.
- Zwei Inkassobüros wurden zur Beitreibung von Geldbeträgen ihr gegenüber beauftragt.
- Ein Mahnbescheid erging wegen rückständiger Miete.
- Ein Mahnbescheid einer Elektrofirma ging ein.
- Ein weiterer Mahnbescheid eines Autohauses wurde zugestellt.

- Auch ein Versandhaus ließ einen Mahnbescheid zustellen.
- Schließlich erging ein Versäumnisurteil.

Es lag eine Personenverwechslung vor. Die Maßnahmen richteten sich gegen eine völlig unbeteiligte Frau.

Da der Name der Frau im Melderegister nur einmal vorhanden war, wurde die in der Anfrage mitgeteilte angebliche frühere Anschrift nicht mit dem Melderegister verglichen. Aufgrund Gleichheit von Name und Vorname wurde die angebliche neue Anschrift bekanntgegeben, ohne daß die Personenverwechslung erkannt worden wäre. Die Stadt fügte nur den obengenannten Hinweis an. Gegenwärtig prüft die Stadt, ob zur Abhilfe eine Änderung des Systems vorgenommen werden könnte.

Ein solcher Fall von Personenverwechslung kann immer wieder passieren – wenn auch nicht immer mit so gravierenden Folgen. Der Fall zeigt, daß Forderungen des Datenschutzes, die zu einem exakteren Umgang mit den einer Behörde anvertrauten personenbezogenen Daten führen würden, auch dem eingangs zitierten Normalbürger, der „nichts zu verbergen" hat, zugute kommen würden. Der Fall macht darüber hinaus ein besonderes Merkmal der Nutzung großer Datensammlungen deutlich, daß nämlich grundsätzlich (aus Rationalisierungsgründen) der Aufwand für die Abwicklung des Einzelfalles – hier für kompliziertere Plausibilitätsprüfungen – gescheut wird. Das gleiche gilt für die Empfänger einer solchen Auskunft, die sich auch durch den von der Stadt routinemäßig angefügten Zusatz „ob Personengleichheit besteht, kann nicht festgestellt werden", von einer Verwendung der neuen Anschrift grundsätzlich nicht abschrecken lassen.

3. Gesundheit

3.1. Krebsregistrierung

Der Bayerische Landtag hat am 23.10.1985 den folgenden Beschluß gefaßt:

„1. Antrag der Abgeordneten Regensburger, Diethei, Böhm u.a. CSU Drs. 10/6471

Krebsregistrierung

2. Antrag der Abgeordneten Heinrich, Warnecke, Kolo u.a. SPD Drs. 10/4314

Einrichtung eines Krebsregisters in Bayern

Die Staatsregierung wird gebeten, darauf hinzuwirken, daß die in Bayern bestehenden universitären Kliniktumorregister (München, Erlangen-Nürnberg, Würzburg) durch Einbeziehung von Daten aus weiteren Bereichen der stationären und ambulanten Behandlung zu wirksamen Instrumenten der Krebserkennung und -bekämpfung ausgebaut werden.

Die Staatsregierung wird weiter gebeten, einen entsprechenden Gesetzentwurf dem Landtag zuzuleiten, falls sich dies im Zuge des Aufbaus der Klinikregister mit Rücksicht auf die ärztliche Schweigepflicht oder aus anderen Gründen als notwendig erweisen sollte.

Die Staatsregierung wird gebeten, bis zum 1. Januar 1986 einen Zwischenbericht zu geben."

Der Landesbeauftragte für den Datenschutz hatte in einer Anhörung der CSU-Fraktion des Bayerischen Landtags zum Thema „Krebsregistrierung" am 1.2.1985 zu den anstehenden Datenschutzfragen das folgende 3-Stufen-Konzept für die Vorgehensweise vorgeschlagen:

1. Definition der von dem Krebsregister zu erbringenden Leistungen (Zieldefinition)
2. Erstellung einer Konzeption – einschließlich eines Datenschutzkonzepts (ärztliche Schweigepflicht) mit Feststellungen über:
   Die verantwortliche speichernde (öffentliche) Stelle,
   die beteiligten Einrichtungen, die Zweckbestimmung
   die Grenzen der Nutzung der personenbezogenen Daten,
   den Umfang der notwendigen Einwilligung sowie
   die technische und organisatorische Sicherstellung der Einhaltung der ärztlichen Schweigepflicht.
3. Entscheidung ob bzw. welche Festlegung in Gesetzesform erfolgen müssen.

Auf die ausführlicheren Darstellungen zum Thema „Krebsregistrierung" im 5. Tätigkeitsbericht (Nr. 4.2) und im 6. Tätigkeitsbericht (Nr. 4.10.1 und 4.10.2 sowie Anhang Nr. 7) darf ich verweisen.

3.2. Erstellen einer Patientenliste für die Polizei

Nach Art. 28 des Bayerischen Meldegesetzes vom 24.3.1983 wird jedermann, der in einem Krankenhaus, Pflegeheim oder in einer ähnlichen Einrichtung aufgenommen wird, in ein Verzeichnis eingetragen, das für die Polizei zur Einsichtnahme bereitzuhalten ist. Abs. 3 der genannten Vorschrift beschränkt den Umfang der Patientendaten in dieser Liste auf den Familiennamen, den gebräuchlichen Vornamen, den Tag und den Ort der Geburt sowie die Anschrift. Anstelle des Verzeichnisses können gemäß Art. 28 Abs. 4 MeldeG auch andere Unterlagen des Krankenhauses treten, wenn sie die vorgenannten Daten enthalten und wenn für die Polizei die Einsichtnahme auf diese Daten beschränkt werden kann. Die Polizei darf diese Daten nur für Zwecke der Gefahrenabwehr oder der Strafverfolgung sowie zur Aufklärung der Schicksale von Vermißten und Unfallopfern auswerten und verarbeiten (Art. 29 Abs. 2 MeldeG).

Bei Überprüfungen habe ich in einem Krankenhaus festgestellt, daß die dort erstellte „Polizeiliste" mehr Daten enthielt, als nach der oben genannten Vorschrift vorgesehen sind. Außerdem stellte sich dort die Frage, ob eine regelmäßige (wöchentliche) Weitergabe der „Polizeiliste" an die Polizei zulässig wäre. Diese Frage ist zu verneinen. Die Polizei hat vielmehr nach Art. 28 MeldeG lediglich die Möglichkeit der Einsichtnahme beim Krankenhaus. Dabei ist noch darauf zu achten, daß bei Ermittlungen wegen Ordnungswidrigkeiten die Polizei nur in Fällen von erheblicher Bedeutung für die Allgemeinheit Einsicht nehmen darf (siehe Nr. 28.4 der Vollzugsbekanntmachung zum Meldegesetz vom 28.4.1984, MABl Seite 186).

Unsicherheiten im Umgang mit dem neuen Melderecht habe ich im Krankenhausbereich nicht nur bei der vorgenannten

Polizeiliste, sondern auch bei der Anmeldung von Patienten festgestellt. Es sei deshalb darauf hingewiesen, daß nach Art. 28 Abs. 1 MeldeG eine Meldepflicht nur für diejenigen Personen besteht, die nicht für eine andere Wohnung innerhalb des Geltungsbereiches des Bundes-Melderechtsrahmengesetzes gemeldet sind. Diese Meldeverpflichtung trifft außerdem grundsätzlich den Patienten selbst. Nur wenn er wegen Gebrechlichkeit seiner Meldepflicht nicht nachkommen kann, hat der Anstaltsleiter bzw. sein Beauftragter die Anmeldung vorzunehmen. Für Entmündigte obliegt die Meldepflicht dem Vormund, für Personen für die ein Pfleger bestellt ist, der den Aufenthalt bestimmen kann, diesem Pfleger. Soweit Krankenhäuser Patienten bei den Meldeämtern anmelden, sind diese Meldungen also auf die genannten Fälle, in denen das Krankenhaus selbst tätig werden kann, zu beschränken. Auch der bei der Meldung verwendete Datenrahmen (Meldeformular) muß den neuen melderechtlichen Vorschriften angepaßt werden.

3.3. Aufbewahrung ärztlicher Aufzeichnungen bei Auflösung einer Arztpraxis ohne Übertragung auf einen Nachfolger

Der Bundesgerichtshof hat die Überlassung von Patientenunterlagen an einen Praxisnachfolger ohne vorherige Befragung der Patienten unter dem Gesichtspunkt der mutmaßlichen Einwilligung für zulässig erachtet (Urteil vom 7.11.1983, NJW 1984 Seite 602). Die Überlassung der Patientenkartei bei Praxisübergabe ist zur weitverbreiteten Praxis geworden. Anders ist die Situation aber möglicherweise, wenn eine Praxis aufgelöst wird, ohne daß eine Übertragung auf einen Praxisnachfolger stattfindet. Hier besteht stets die Gefahr, daß die Krankenunterlagen etwa auf Veranlassung der Erben an einen für den Patienten nicht ohne weiteres feststellbaren Ort gelangen, an dem sie möglicherweise unbeaufsichtigt und dem Zugriff unbefugter Dritter ausgesetzt sind. Es ist jedoch davon auszugehen, daß die Patienten in der Regel ein Interesse daran haben, daß die Unterlagen nach einer Praxisaufgabe „in gehörige Obhut gegeben werden" (vergl. auch § 11 Abs. 4 der Berufsordnung für die Ärzte Bayerns in der Fassung vom 1.10.1983). Das Bayerische Staatsministerium des Innern hat zu dieser Frage die Ansicht vertreten, daß auch eine Aufbewahrung von Patientenunterlagen durch besonders verpflichtete Mitarbeiter eines privaten Archivunternehmens dem wohlverstandenen Interesse der Patienten entspreche. Eine (mutmaßliche) Einwilligung der Patienten könne freilich nur vermutet werden, wenn die Mitarbeiter des privaten Archivunternehmens vertraglich zur Verschwiegenheit verpflichtet worden seien oder wenn die Archivierung und Verwaltung der Unterlagen von vornherein einem Arzt vorbehalten sei, der schon kraft Gesetzes zur Verschwiegenheit verpflichtet ist.

Diese Auffassung zur Abgabe ärztlicher Aufzeichnungen an ein privates Archiv bei Auflösung einer Arztpraxis halte ich nicht für völlig bedenkenfrei. Der BGH hat in der angeführten Entscheidung ausgeführt: „Die Überlassung der Behandlungsunterlagen liegt nämlich im Regelfall im Interesse des einzelnen Patienten und entspricht seinem mutmaßlichen Willen: Dem Praxisnachfolger wird für eine etwaige spätere Behandlung wertvolles Material zur Diagnose und Therapie an die Hand gegeben, wenn der Patient nach dem Praxiswechsel ihn aufsucht". Dies trifft jedoch den hier zu entscheidenden Fall nicht. Bei Abgaben ärztlicher Aufzeichnungen bei Auflösung einer Arztpraxis ohne Praxisnachfolger steht nicht eine Erleichterung für die mögliche Weiterbehandlung des Patienten durch einen anderen Arzt im Vordergrund, sondern die Erfüllung von Aufbewahrungspflichten, wie sie etwa in § 11 Abs. 2 und 4 der Berufsordnung für die Ärzte Bayerns vorgesehen sind. Der Umstand, daß die Verwaltung der Unterlagen in einem privaten Archivunternehmen von einem Arzt vorgenommen werden soll, mag in diesem Zusammenhang Bedeutung für die Frage der Zuverlässigkeit und Fachkunde haben. Es ist jedoch davon auszugehen, daß der Genannte in diesen Fällen Unterlagen nicht in seiner Eigenschaft als – in die Behandlung eintretender – Arzt erhält. Damit ist in Frage gestellt, ob auf diese Person § 203 Abs. 1 Nr. 1 StGB (also die Strafandrohung bei Verletzung der Schweigepflicht) zutrifft, bzw. ob und inwieweit diese Vorschrift Anwendung findet. Zu prüfen wäre außerdem, ob durch die Angabe der Unterlagen eine Schutzwirkung aus den §§ 53 Abs. 1 Nr. 3, 53 a, 76, 97 Abs. 1 und 2 StPO – soweit eine solche existiert – verloren ginge, ob also die Übertragung an ein privates Archivunternehmen das Herauslösen der Unterlagen aus dem vom Zugriff Dritter geschützten ärztlichen Bereich bedeuten würde.

Meines Erachtens sollte trotz allen rechtlichen Schwierigkeiten eine Lösung gesucht werden, die dem wohlverstandenen Interesse der Patienten gerecht wird. Dabei sollte der Gedanke aufgegriffen werden, daß in der neueren Gesetzgebung und im Verwaltungsvollzug zum Datenschutzrecht zunehmend die Tendenz erkennbar wird, privaten Stellen den Umgang mit besonders sensiblen Daten im Auftrag einer zu besonderen Verschwiegenheit verpflichteten öffentlichen Stelle nur dann zu erlauben, wenn die Aufgabenerfüllung anders nicht möglich wäre (vergl. § 80 Abs. 5 SGB X und Vollzugsbekanntmachung Nr. 3.3 zu Art. 3 BayDSG). Ich habe daher auf Art. 2 Abs. 1 Kammergesetz hingewiesen, wonach die Berufsvertretung (bestehend aus den Ärztlichen Kreisverbänden, den Ärztlichen Bezirksverbänden und der Landesärztekammer) die Aufgabe hat, im Rahmen der Gesetze die beruflichen Belange der Ärzte wahrzunehmen und die Erfüllung der ärztlichen Berufspflichten zu überwachen. Ich habe die Auffassung vertreten, daß im Rahmen dieser Aufgabenzuweisung zunächst zu prüfen wäre, ob die Aufbewahrung ärztlicher Aufzeichnungen bei Auflösung einer Arztpraxis ohne Praxisnachfolger nicht durch die Berufsvertretungen erfolgen könnte. Eine solche Lösung hätte u.a. auch den Vorteil, daß die eventuell notwendig werdende Suche nach dem Fundort von Patientenunterlagen aus aufgelösten Arztpraxen erheblich vereinfacht würde. Erst wenn die Berufsvertretung nachweisen würde, daß ihr der Vollzug dieser Aufgaben aus einem wichtigen Grund nicht zugemutet werden könne, sollte erwogen werden, unter welchen Bedingungen die Aufbewahrung ärztlicher Aufzeichnungen bei einem privaten Archivunternehmen zulässig sein könnte. Auch sollte in letzterem Falle sichergestellt sein, daß die Berufsvertretung jederzeit berechtigt ist, die Einhaltung der Vorschriften über die ärztliche Schweigepflicht, den Datenschutz und ergänzende Weisungen bei einem solchen Archivunternehmen zu überwachen.

Die Bayerische Landesärztekammer hat inzwischen mitgeteilt, sie sei nicht bereit die ärztlichen Aufzeichnungen bei Auflösung einer Arztpraxis ohne Praxisnachfolger selbst

aufzubewahren. Sie verweist dabei auf „Grundsätze zur Aufbewahrung von Praxisunterlagen bei Praxisaufgaben", die von der Bundesärztekammer erarbeitet und angenommen wurden. Danach wird die Übergabe von Praxisunterlagen an ein privates Archivunternehmen für zulässig erachtet, wenn dessen Mitarbeiter vertraglich zur Verschwiegenheit verpflichtet sind und die Auskunftserteilung aus den Arztaufzeichnungen einem Arzt vorbehalten ist. Grundvoraussetzung sei außerdem, daß dem Arzt selbst die Aufbewahrung nicht zumutbar, eine Übergabe an den Praxisnachfolger nicht möglich sei und die Ärztekammer die Aufbewahrung nicht übernehme. Die Ärztekammer wird die Ärzteschaft auf die Möglichkeit der Aufbewahrung durch ein privates Unternehmen hinweisen, wenn das Unternehmen eine schriftliche Erklärung vorlege, daß die für Ärzte geltende Schweigepflicht unbedingt beachtet werde.

Das Bayerische Staatsministerium des Innern weist in einer Stellungnahme hierzu darauf hin, daß eine Verpflichtung der Berufsvertretung zur Aufbewahrung ärztlicher Aufzeichnungen aus Art. 2 Abs. 1 des Kammergesetzes nicht abgeleitet werden könne. Der von der Landesärztekammer gewählte Weg wurde unter dem Gesichtpunkt der mutmaßlichen Einwilligung rechtlich für zulässig und im Interesse eines möglichst effektiven Schutzes der Patientenunterlagen vor dem Zugriff unbefugter Dritte auch für zweckmäßig gehalten. Ich habe nach wie vor Zweifel daran, ob die Übergabe personenbezogener Patientenunterlagen an ein privates Archivunternehmen die beste mögliche Lösung darstellt. Die Zweifel sind im wesentlichen in der geringen Kontrollierbarkeit des Umgangs mit den Daten bei den privaten Unternehmen und in dem oben dargestellten Umstand zu sehen, daß die Angaben bei den Unternehmen möglicherweise keinen ausreichenden rechtlichen Schutz vor Zugriff anderer Stellen unterliegen.

3.4. Erhebung von Personal-Gesundheitsdaten bei Dritten

Ein früher verwendeter Fragebogen des Gemeindeunfallversicherungsverbandes sah im Fall von Hepatitiserkrankungen vor, beim Erkrankten mit einem Fragebogen personenbezogene Daten über Dritte, beispielsweise Patienten oder Arbeitskollegen, mit denen er in Kontakt gekommen war, zu erheben. In einem Hinweis von ärztlicher Seite, den ich erhielt, wurde der Fragebogen für zu weitgehend erachtet. Gegenüber dem Gemeindeunfallversicherungsverband habe ich gegen die personenbezogene Datenerhebung über Dritte Bedenken angemeldet, da Nachforschungen über die Art der Erkrankung Dritter bei Rücksichtnahme auf die ärztliche Schweigepflicht ohnehin eine Entbindung entwaiger Auskunftsgeber durch den Betroffenen voraussetzen (§ 203 StGB, Art. 13 Abs. 5 Bayer. Krankenhausgesetz). Im vorliegenden Fall kam es jedoch darauf an, für die Anerkennung einer Hepatitis als Berufskrankheit im Sinne der gesetzlichen Unfallversicherung den Nachweis einer durch die Berufstätigkeit über das normale Maß hinausgehende Ansteckungsgefahr zu führen. Ich gab zu bedenken, daß dieser Nachweis auch ohne Offenbarung personenbezogener Daten über Dritte durch eine entsprechende Bescheinigung des Arbeitgebers geführt werden könne, die eine Identifikation der dritten Personen vermeidet. Der Bayer. Gemeindeunfallversicherungsverband hat den Fragebogen daraufhin überarbeitet. Die Frage nach Kontaktpersonen ist darin nicht mehr enthalten.

3.5. Datenerhebung über Ärzte und anderes Klinikpersonal

Durch eine Klinik wurde ich darauf aufmerksam gemacht, daß ein Gesundheitsamt regelmäßig im Zusammenhang mit der Erhebung von Daten für den Jahresgesundheitsbericht von Krankenhäusern seines Einzugsbereichs listenmäßige Aufstellungen über Namen, Geburtsdatum, Anschrift und teilweise auch Prüfungsdatum der in den Krankenhäusern beschäftigten Medizinalpersonen anfordere. Aufgrund meiner Überprüfung habe ich den Sachverhalt folgendermaßen beurteilt:

Zur Erstellung des Jahresgesundheitsberichts ist aus der Sicht des Datenschutzes eine personenbezogene Erhebung von Daten über Ärzte und andere Berufe des Gesundheitsdienstes nicht erforderlich. Dies ergibt sich schon aus der Natur des Jahresgesundheitsberichts, der ein Tätigkeitsbericht der Gesundheitsämter sein soll und deshalb nur aggregierte Daten zu enthalten braucht. Die Erhebung von Daten zur Erstellung des Berichts braucht sich deshalb nicht auf personenbezogene Daten über Ärzte und andere im Gesundheitswesen tätigen Personen zu beziehen.

Davon zu unterscheiden sind die dem Gesundheitsamt im Rahmen der Medizinalaufsicht obliegenden Aufgaben. Die Notwendigkeit einer namentlichen Erfassung von Ärzten und medizinischem Hilfspersonal durch die Gesundheitsämter im Rahmen der Medizinalaufsicht wird von mir nicht angezweifelt, soweit eine gesetzliche Meldepflicht dieser Personen gegenüber dem Gesundheitsamt besteht. Die gesetzliche Meldepflicht nach Art. 4 Abs. 6 des Kammergesetzes verpflichtet die Medizinalpersonen selbst. Diese Verpflichtung kann allerdings nicht ohne weiteres durch eine regelmäßige und listenmäßige Datenoffenbarung durch die Arbeitgeber ersetzt werden. Will der Arbeitgeber (z.B. die Klinik) diese Meldeverpflichtung aus Praktikabilitätsgründen übernehmen, bedarf es hierzu der Einwilligung der Betroffenen. Dabei ist zu beachten, daß dann der Datenumfang auf das erforderliche Minimum zu beschränken ist.

Eine andere Beurteilung kann ich auch Art. 2 Abs. 2 Kammergesetz nicht entnehmen, wonach eine Berufsvertretung berechtigt ist, innerhalb ihres Aufgabenbereichs Anfragen an die zuständigen Behörden zu richten. Diese Vorschrift kann die – in einem anderen mir bekanntgewordenen Falle – vom Ärztlichen Kreis- und Bezirksverband gewünschte Datenoffenbarung durch den Arbeitgeber ohne Einwilligung der Betroffenen meines Erachtens nicht rechtfertigen. Zum einem nennt Art. 2 Abs. 2 Kammergesetz hier Behörden generell also Ansprechpartner, nicht in ihrer besonderen Eigenschaft als Arbeitgeber. Würde Art. 2 Abs. 2 die gewünschte Datenoffenbarung zulassen, würde dies darüber hinaus auch zu einer Ungleichbehandlung des ärztlichen Personals in Privatkliniken einerseits und dem Medizinalpersonal, das in Krankenhäusern öffentlicher Träger tätig ist, führen. Zum anderen ergibt sich auch aus Art. 2 Abs. 2 Kammergesetz die Einschränkung, daß Behörden der Berufsvertretungen auf Anfragen Auskunft erteilen sollten, soweit nicht dienstliche Gründe entgegenstehen. Vorliegend steht einer Datenoffenbarung grundsätzlich das Personalaktengeheimnis entgegen. Außerdem wäre Art. 2 Abs. 2 Kammergesetz wohl kaum eine hinreichend

normenklare bereichsspezifische Datenübermittlungsvorschrift im Sinne der Rechtsprechung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983.

3.6. Weitergabe von Arztbriefen an Sozialpsychiatrische Dienste

Aufgrund der Eingabe einer Patientin hatte ich die Frage zu klären, ob und inwieweit Nerven-Krankenhäuser Arztbriefe an Sozialpsychiatrische Dienste weitergeben dürfen. Ich habe hierzu folgende Ansicht vertreten:

Die Weitergabe von Arztbriefen vom Krankenhaus an Sozialpsychiatrische Dienste ist nach Art. 13 Abs. 5 Bayerisches Krankenhausgesetz nur zulässig, wenn der Patient zustimmt. Die Zustimmung kann nach herrschender Meinung auch mündlich oder im Rahmen einer konkludenten Einwilligung erfolgen; wegen der damit verbundenen Beweisschwierigkeiten im Streitfall ist jedoch der Schriftform der Vorzug zu geben. Im Hinblick auf die Problematik einer möglicherweise eingeschränkten Einsichtsfähigkeit des Patienten sollte jedoch sorgfältig darauf geachtet werden, daß nur das Minimum der unbedingt erforderlichen Angaben an die Sozialpsychiatrischen Dienste weitergegeben wird. Die Übersendung eines abschließenden Arztbriefes kommt in diesem Zusammenhang nur dann in Frage, wenn ein Arzt im Sozialpsychiatrischen Dienst die Nachbehandlung des Patienten übernimmt. Nach meinem Kenntnisstand beschränkt sich die Aufgabe der Ärzte in den Sozialpsychiatrischen Diensten gegenwärtig auf beratende Funktionen. Der Übersendung eines vollständigen Arztbriefes mit seinen vielfach sehr sensiblen Informationen an den Sozialpsychiatrischen Dienst ist daher in diesen Fällen nicht vertretbar. Im Rahmen der Einwilligung sind die Mitteilungen vielmehr auf die Angaben zu beschränken, die für die begleitende oder nachsorgende Betreuung der psychisch Kranken unbedingt erforderlich sind.

Die zwischenzeitlich erlassenen Richtlinien des Bayer. Staatsministeriums für Arbeit und Sozialordnung über die Aufgaben der Sozialpsychiatrischen Dienste haben mich in meiner Auffassung bestätigt.

3.7. Hinweis auf die Freiwilligkeit bei der Erhebung von Gesundheitsdaten

Das Bayerische Staatsministerium für Arbeit und Sozialordnung stellte für Ermittlungen eines bestimmten Schwermetallgehalts im Blut in einem Fragebogen Fragen über Wohngegend, Berufstätigkeit, durchgemachte Krankheiten und Rauchgewohnheiten an eine größere Zahl von Personen. Die Daten wurden so erhoben, daß ein Rückschluß auf bestimmte Personen nicht ausgeschlossen war. In einem besonderen Schreiben, das den Betroffenen ausgehändigt wurde, ist die Bitte enthalten, die Untersuchung des Blutes durchführen zu dürfen. Außerdem wird darin um Verständnis für die im Fragebogen gestellten Fragen geworben. Ein ausdrücklicher Hinweis auf die Freiwilligkeit der Datenerhebung fehlte jedoch:

Ich habe das Ministerium gebeten, entsprechend Art. 16 Abs. 2 BayDSG auf die Freiwilligkeit der Angabe von Daten ausdrücklich hinzuweisen und zu bedenken gegeben, daß die Betroffenen nicht erkennen können, ob das Schreiben eine „bürgerfreundliche" Aufforderung enthält, einer gesetzlichen Pflicht nachzukommen, oder die Bitte um eine freiwillige Teilnahme.

Das Ministerium war der Ansicht, daß die in dem Schreiben ausgesprochene Bitte und das Werben um Verständnis für die Notwendigkeit der Fragen als Hinweis auf die Tatsache der Freiwilligkeit zu werten sei. Außerdem versicherte es, daß der mit der Durchführung der Aktion betraute Arzt, der bei den Untersuchungen anwesend ist, die Probanden mündlich auf die Freiwilligkeit der Teilnahme hinweist.

Ich würde über diesen Vorgang nicht berichten, wenn es sich um einen seltenen Einzelfall handeln würde. Meiner Erfahrung nach betrifft er jedoch einen typischen Sachverhalt, den ich auch in den vergangenen Jahren wiederholt bemerkt habe: Es ist immer wieder festzustellen, daß freiwillige Datenerhebungen dem Betroffenen in einer Weise nahegebracht werden, die ein Nichtsachkundiger kaum von einer freundlichen „Verpackung" einer gesetzlich bestehenden Pflicht unterscheiden kann. In manchen Fällen – nicht in dem oben geschilderten Fall, wenn ein Arzt selbst auf die Freiwilligkeit hinweist – werden derartige Formulierungen gewählt, um die Rücklaufquote, d.h. die Zahl der verwertbaren Antworten, auf die freiwillige Anfrage zu erhöhen. Ich bin der Ansicht, daß eine solche Verfahrensweise der gesetzlich gebotenen Hinweispflicht und damit auch der Transparenz der Datenverarbeitung widerspricht. Soweit es den Fragestellern bei einem ausdrücklichen Hinweis auf die Freiwilligkeit nicht gleichwohl gelingt, ausreichend Verständnis für die freiwillige Abgabe der Daten zu erwecken, halte ich es für ein unzulässiges Mittel, die Frage, ob Verpflichtung oder Freiwilligkeit, soweit offen zu halten, daß die überwiegend staatstreuen Mitbürger vorsorglich Angaben machen, um nur einer eventuell bestehenden Verpflichtung nicht zuwider zu handeln.

3.8. Anfragen von Krankenhäusern bei Meldeämtern

Eine Klinik hatte zu Anfragen bei Meldeämtern zur Feststellung des Aufenthaltsortes von Patienten ein Formblatt verwendet, in dem gegenüber den Meldeämtern Angaben über die Krankheit und den Zeitpunkt einer histologischen Untersuchung des betroffenen Patienten gemacht wurden. Ich habe die Klinik darauf hingewiesen, daß solche Angaben gemäß Art. 13 des Bayerischen Krankenhausgesetzes bzw. § 203 StGB unter die ärztliche Schweigepflicht fallen und auch für die erbetene Auskunft nicht erforderlich sind. Ich habe vorgeschlagen, für das Auskunftsersuchen eine neutralere Form zu wählen. Dabei habe ich auch gebeten, zu prüfen, ob im Briefkopf des Anschreibens die Bezeichnung „Abteilung für Knochenmarksdiagnostik" entfallen oder durch eine neutrale Abteilungsnummer ersetzt werden könnte. Ein solcher indirekter Hinweis auf die Art der Erkrankung ist für die Prüfung der Zulässigkeit einer Auskunft aus dem Melderegister m.E. nicht erforderlich.

Die Klinik hat meinem Vorschlag entsprochen.

3.9. Fertigung von Fotografien bei der Patientenaufnahme in Bezirkskrankenhäusern

Aufgrund der Beschwerde eines Betroffenen habe ich festgestellt, daß bei der Patientenaufnahme in einem Bezirkskrankenhaus stets Fotografien von dem Betroffenen gefertigt wurden. Dies geschah auch dann, wenn der Patient sich freiwillig in Behandlung begeben hatte.

In der von mir erbetenen Stellungnahme hat das Bezirkskrankenhaus ausgeführt, daß Fotografien des Gesichtsausdrucks psychisch Kranker „im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich seien" (Art. 13 Abs. 2 Bayerisches Krankenhausgesetz). Da die Fotos fester Bestandteil der Krankengeschichte sind, sei der Zugriff auf sie bzw. ihre Weitergabe nur mit ausdrücklicher Zustimmung des Patienten oder seines gesetzlichen Vertreters zulässig. Das Bayerische Staatsministerium für Arbeit und Sozialordnung hat in einer Stellungnahme die regelmäßig durchgeführten Fotografien im klinischen Bereich der Bezirkskrankenhäuser als grundsätzlich notwendig angesehen.

Eine stichprobenweise Umfrage bei den Nervenkrankenhäusern anderer Bundesländer durch die zuständigen Landesbeauftragten hat ergeben, daß die Fertigung von Fotografien bei der Patientenaufnahme im Regelfall nicht erfolgt. Daraufhin habe ich mich an den Verband der Bayerischen Bezirke mit der Bitte um Mitteilung gewandt, in welchen bayerischen Bezirkskrankenhäusern in gleicher Weise verfahren wird und auf die Schwierigkeiten bei der Erlangung der Einwilligung des Patienten hingewiesen. Daraufhin hat mir der Verband der Bayerischen Bezirke die Empfehlung seines Fachausschusses für Psychiatrie mitgeteilt, wonach künftig von einem Fotografieren der Patienten bei der Aufnahme in Bezirksnervenkrankenhäusern Abstand genommen werden soll, sofern nicht besondere Umstände dies rechtfertigen. Mit dem Verzicht auf die regelmäßige Anfertigung von Fotografien werden meines Erachtens mehrere ungelöste datenschutzrechtliche Probleme beseitigt. Patientendaten, zu denen auch – ähnlich wie Röntgenbilder – Fotografien zählen, dürfen nach Art. 13 Abs. 2 Bayerisches Krankenhausgesetz vom Krankenhaus nur gespeichert werden, soweit dies zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich ist. Der Umstand, daß die regelmäßige Fertigung von Fotografien bei der Patientenaufnahme nur von einem Teil der bayerischen Bezirksnervenkrankenhäuser vorgenommen wird und außerbayerische Nervenkrankenhäuser ebenfalls weitgehend darauf verzichten, deutet daraufhin, daß auch von Fachseite eine solche Verfahrensweise nicht in jedem Fall für erforderlich gehalten wird. Dies wiederum muß Zweifel an der Zulässigkeit einer regelmäßigen Dokumentation des Gesichtsausdrucks psychisch Kranker wecken. Das Bayerische Staatsministerium für Arbeit und Sozialordnung hat in seiner Stellungnahme ausgeführt, „daß selbstverständlich davon ausgegangen wird, daß schon als Ausfluß des Persönlichkeitsrechts Fotoaufnahmen ausschließlich mit Zustimmung des Patienten oder des gesetzlichen Vertreters gemacht werden." Dies wird im Hinblick auf die geistige und seelische Verfassung mancher Patienten nicht unproblematisch sein.

In begründeten Fällen kann die Anfertigung von Fotografien erforderlich im Sinne des Art. 13 Abs. 2 Bayerisches Krankenhausgesetz sein.

3.10. Anforderung von Krankenunterlagen durch ein Versorgungsamt

Aufgrund einer Anfrage war zu klären, in welchem Umfang ein Krankenhaus einem Versorgungsamt Einblick in die Krankengeschichte geben darf. Das Bayerische Staatsministerium für Arbeit und Sozialordnung hat dazu die folgende Ansicht vertreten, die von mir geteilt wird:

Bei Auskünften und Übersendungen von Akten (Krankengeschichten) an Landesversicherungsanstalten, Versorgungsämter, Gerichte, Ausführungsbehörden für gesetzliche Unfallversicherung bei Gemeinden, bei Gemeindeverbänden, Ländern, der Bundesbahn, der Bundespost und der Berufsgenossenschaften, Gesundheitsämtern und Krankenhäusern ist grundsätzlich die Einwilligung des Patienten selbst einzuholen. Für den Nachweis des Vorliegens der Einwilligung genügt in diesen Fällen eine entsprechende Versicherung dieser Stellen; die Versicherung sollte allerdings möglichst den Wortlaut der Einwilligung enthalten, damit der Umfang der Einwilligung geprüft werden kann. Alle übrigen ersuchenden Stellen haben das Einvernehmen des Patienten urschriftlich nachzuweisen. Einsicht in Krankengeschichten darf, soweit im Einzelfall die Gewährung der Einsicht gestattet ist, nur Ärzten gewährt werden, die für die vorgenannten Stellen tätig sind. Vor Aushändigung oder Gewährung der Einsicht ist trotz Einwilligung die Krankengeschichte vom behandelnden leitenden Krankenhausarzt daraufhin zu überprüfen, ob die Herausgabe oder Gestattung der Einsicht dem Interesse des Patienten entspricht. Trifft dies nicht zu oder besteht sonst ein wichtiger Grund, die Aushändigung der Krankheitsgeschichte oder die Einsicht in sie zu verweigern, kann dem Auskunftsersuchen nur in Form eines schriftlichen oder mündlichen Berichts entsprochen werden.

Die zu erteilende Auskunft hat das zu enthalten, worauf der Ersuchende einen Rechtsanspruch hat. Sie kann in Form von Auszügen aus der Krankheitsgeschichte oder in Form von Gutachten erteilt werden, vorausgesetzt, daß diese nicht mehr enthalten als der Beteiligte erfahren darf. Bei auskunftsberechtigten Behörden und Stellen sind stets Art und Umfang der Auskunft, welche die einschlägige Rechtsnorm gewährt, zu prüfen. Die Auskunft darf nur in dem so festgestellten Rahmen erteilt werden. Zusammenfassend kann also festgestellt werden, daß die letztendliche Verantwortung für Herausgabe, Einsichtnahme oder Auskunft aus der Krankengeschichte bei dem leitenden Krankenhausarzt liegt.

Ergänzend zu dieser Stellungnahme des Staatsministeriums für Arbeit und Sozialordnung ist darauf hinzuweisen, daß als Rechtsgrundlage für diese Auffassung Art. 13 Abs. 5 des Bayerischen Krankenhausgesetzes heranzuziehen ist. Es ist klarzustellen, daß die Krankenhausverwaltung gespeicherte Patientendaten nur weitergeben darf, soweit dies zur verwaltungsmäßigen Abwicklung der Behandlung des Patienten erforderlich ist (Art. 13 Abs. 4 Bayer. Krankenhausgesetz). Die Übersendung von Krankengeschichten wird regelmäßig nicht dazu zählen. Durch geeignete organisatorische Maßnahmen im Krankenhaus ist daher

meines Erachten sicherzustellen, daß Ersuchen über die Auskunft aus Krankenunterlagen dem leitenden Krankenhausarzt zur Entscheidung vorgelegt werden. Das Versorgungsamt habe ich gebeten, die Anforderung von Krankenunterlagen nicht an die jeweilige Krankenhausverwaltung, sondern an den leitenden Chefarzt des Krankenhauses zu richten.

3.11. Schreibdienstuntersuchung in einem Krankenhaus

Aufgrund einer Eingabe hatte ich mich mit der Frage der Einhaltung der ärztlichen Schweigepflicht bei einer Wirtschaftlichkeitsuntersuchung über den Schreibdienst in einem Krankenhaus zu befassen. Ich habe mich dazu folgendermaßen geäußert:

Die Weiterleitung von Patientendaten durch das Krankenhaus an die Organisationsstelle des Landratsamtes beurteilt sich nicht unmittelbar nach den Vorschriften des Bayerischen Datenschutzgesetzes, da es sich nicht um eine Datenübermittlung aus einer Datei gemäß Art. 5 Abs. 3 Ziffer BayDSG handelt und darüber hinaus besondere Vorschriften über die Verschwiegenheitspflichten den Vorschriften des Bayerischen Datenschutzgesetzes vorgehen. Eine solche Vorschrift stellen § 203 StGB sowie Art. 13 des Bayerischen Krankenhausgesetzes dar.

Das Übermittlungsersuchen des Landratsamtes zielte nun aber nicht auf die Übermittlung von Patientendaten ab, sondern sollte für eine Untersuchung Aufschluß darüber bringen, ob und ggf. mit welchen Mitteln der Schreibdienst des Krankenhauses rationeller organisiert werden könnte. Hierzu hat das Landratsamt im Rahmen des Art. 51 Abs. 3 Nr. 1 der Bayerischen Landkreisordnung das Organisationsrecht. Dieses muß allerdings im Rahmen des Grundsatzes der Gesetzmäßigkeit der Verwaltung ausgeübt werden. Organisationsmaßnahmen dürfen keinen Eingriffscharakter haben und müssen den Verfassungsgeboten der Verhältnismäßigkeit des Übermaßverbotes Rechnung tragen.

Als Lösung habe ich in diesem Fall vorgeschlagen, auf den zu untersuchenden Schriftstücken die Patientennamen sowie Geburtsdatum und Anschrift zu schwärzen. Dies dürfte im Regelfall ausreichen, um den Geheimnisschutz zu wahren. Soweit jedoch auch ohne Kenntnis der vorgenannten Daten aus den anamnestischen Angaben sowie entsprechenden Untersuchungsbefunden Rückschlüsse auf bestimmte Patienten gezogen werden könnten, wären auch diese Daten zu schwärzen. Zu einer Identifizierung können nämlich grundsätzlich neben dem Namen auch andere Patientendaten führen. Die Entscheidung, welche Patientendaten im Einzelfall zu schwärzen sind, obliegt dem ärztlichen Dienst des Krankenhauses, nicht der Organisationsstelle des Landratsamts.

3.12. Offenbarung von Patientendaten durch ein Krankenhaus gegenüber einer Sparkasse

In einer Eingabe wurde ich darauf hingewiesen, daß ein Krankenhaus während einiger Jahre der örtlichen Sparkasse Informationen über Patienten (Namen und die Tatsache des Aufenthalts im Krankenhaus) zugängig gemacht hat. Diese Praxis wurde auf Weisung des zuständigen Landratsamtes bereits vor meiner Befassung mit dieser Angelegenheit eingestellt. Die Weitergabe der Patientendaten verstieß gegen Art. 13 Abs. 4 und 5 des Bayerischen Krankenhausgesetzes. Die Sparkasse hat die Informationen über den Krankenhausaufenthalt der betroffenen Patienten für Zwekke der Kundenbetreuung genutzt. Die Datenweitergabe war somit nicht zur Abwicklung der Behandlung der Patienten erforderlich. Auch lag eine rechtswirksame Einwilligung der Patienten nicht vor.

Ich habe in diesem Fall empfohlen, im Rahmen einer Schulung der Mitarbeiter auf die Einhaltung der datenschutzrechtlichen Bestimmung im Krankenhaus hinzuwirken.

3.13. Erstellung einer Patientenstrukturanalyse durch eine Beratungsgesellschaft

Durch Hinweise habe ich davon erfahren, daß eine Beratungsgesellschaft im Auftrag der Bayerischen Bezirke eine Patientenstrukturanalyse in bayerischen Bezirkskrankenhäusern durchführte. Dies habe ich zum Anlaß genommen, die dabei verwendeten Fragebogen zu überprüfen. Die Fragen sollten dazu dienen, die näheren Umstände des Krankenhausaufenthalts der einzelnen Patienten zu erheben. Da die Zustimmung des Patienten nicht vorgesehen war, kam nur eine solche Weitergabe von Daten an die Beratungsgesellschaft in Frage, bei der der Patient durch die Weitergabe nicht identifiziert werden konnte. Der Fragebogen enthielt keine Angaben über Namen und Anschrift der Patienten. Es waren daher die übrigen Daten darauf zu überprüfen, ob sie unter Zuhilfenahme zusätzlicher Informationen bei der Beratungsgesellschaft zu einer Identifizierung der Betroffenen unschwer führen könnten. Als Ergebnis der Überprüfung habe ich gebeten, die Bezeichnung des Wohnorts nicht mitzuerfassen, da insbesondere bei kleineren Gemeinden eine Identifizierung des Patienten möglich erschien. Außerdem habe ich die Auffassung vertreten, daß die Speicherung der chiffrierten laufenden Patientennummer auf den unbedingt erforderlichen Zeitraum zu beschränken sei. Spätestens nach der Plausibilitätsprüfung der erfaßten Fälle wären die Patientennummern zu löschen und die Fragebogen an die Krankenhäuser zurückzusenden. Von einer Speicherung der Patientennummer in der bereinigten Stammdatei bat ich abzusehen.

3.14. Nutzung von Ärzteanschriften für Wahlwerbung

Ein Ärztlicher Kreisverband hatte im März 1984 auf Bitte eines Mitgliedes im Hinblick auf damals anstehende Kommunalwahlen Briefe mit wahlwerbendem Inhalt an Ärzte versandt. Dabei wurden die beim Verband im Hinblick auf die Mitgliedschaften nach Art. 4 Kammergesetz gespeicherten Anschriften der Ärzte im Zuständigkeitsbereich genutzt. Eine Übermittlung der Daten an Dritte fand in diesem Zusammenhang jedoch nicht statt. Die Datennutzung zu Zwecken der Wahlwerbung war im Hinblick auf Art. 14 Abs. 1 BayDSG zu beanstanden. Nach dieser Vorschrift ist es den bei der Datenverarbeitung beschäftigten Personen untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als den zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu nutzen. Das Bayerische Staatsministerium des Innern, das aufgrund der

beim Landesbeauftragten eingegangenen Eingabe gehört wurde, vertrat die Auffassung, daß der Ärztliche Kreisverband mit der Unterstützung eines seiner Mitglieder anläßlich der Kommunalwahlen den der Berufsvertretung gesetzlich zugewiesenen Aufgabenbereich verlassen hatte. Auch bei großzügiger Betrachtungsweise gehörte es nach Meinung des Ministeriums nicht zu den Aufgaben der Berufsvertretung, die Wahl eines ihrer Mitglieder in ein politisches Gremium durch Versand von Wahlwerbung zu fördern. Es fehlte insoweit an dem konkreten gesundheits- oder berufspolitischen Bezug, den Art. 2 Abs. 1 Kammergesetz für ein Tätigwerden der Berufsvertretung voraussetzt.

4. Sozialbehörden

4.1. Suche nach Unterhaltspflichtigen – unter Verwendung eines problematischen Mittels

Bis vor kurzem wurde als Beilage zu dem Periodicum „Der Amtsvormund" ein „Suchblatt" des Deutschen Instituts für Vormundschaftswesen herausgegeben. Es enthielt jeweils eine Vielzahl von „Unterhaltspflichtigen, Kindsmüttern und Mündeln" – so die Entschließung des Bayerischen Staatsministerims des Innern vom 14.9.1954 (MABl. S.863), nach welcher es von den Jugendämtern den Meldebehörden zur Durchsicht zuzuleiten war. Die Meldebehörden sollten die notwendigen Nachforschungen anstellen und den ausschreibenden Stellen die Ermittlungen von ausgeschriebenen Personen mitteilen. Das Suchblatt enthielt Namen, Vornamen, in manchen Fällen einen Beruf, den Geburtstag und -ort sowie in der Regel das Jugendamt oder auch ein Krankenhaus, das die Person suchte. Die Folge 244 des Suchblatts vom 1.6.1983 enthielt beispielsweise 294 Namen aus dem Bereich der gesamten Bundesrepublik.

Ausgehend von der Klarstellung, daß die Tätigkeit des Jugendamts als Amtsvormund oder Amtspfleger nach den §§ 37 ff des JWG i.V.m. Art. II § 1 Nr. 16 SGB I als eine gesetzliche Aufgabe des Jugendamtes nach dem Sozialgesetz anzusehen ist, formulierte die Datenschutzkommission Rheinland-Pfalz die rechtliche Problematik des vorgenannten Verfahrens folgendermaßen: „Die Datenschutzkommission sieht in den §§ 69 und 74 SGB X keine Rechtsgrundlage für die Offenbarung. Sie vertritt die Auffassung, daß die Maßnahme nicht erforderlich ist und dem Grundsatz der Verhältnismäßigkeit, dem Verfassungsrang zukommt, widerspricht. Die im Belieben einer Behörde oder sonstigen Stelle stehende, an keinerlei besonderen Zulässigkeitsvoraussetzungen oder Prüfungsverfahren gebundene öffentliche Bekanntmachung von Personen, die zum Zwecke der Feststellung der Vaterschaft oder zur Geltendmachung von Unterhaltsansprüchen gesucht werden, kann kein angemessenes Mittel zur Erreichung des mit der Herausgabe des Suchblattes verfolgten Zweckes darstellen. Dabei fällt auch ins Gewicht, daß die Ursache der Ausschreibung der gesuchten Person noch in keinem rechtsförmlichen Verfahren festgestellt wurde."

Die Datenschutzkommission hatte u.a. auch festgestellt, daß die Trefferquote als Folge der Übersendung des Suchblatts an die Meldebehörden offenbar äußerst gering war – sei es, daß sich die gesuchten Personen bei ihrem zuständigen Meldeamt nicht gemeldet hatten, sei es daß das Verfahren aus anderen Gründen nicht funktionierte.

Ich habe das Bayerische Staatsministerium für Arbeit und Sozialordnung von der vorstehend geschilderten Rechtsauffassung unterrichtet und vorgeschlagen, das Suchblattverfahren in Bayern endgültig einzustellen. Das Ministerium hat mir daraufhin mitgeteilt: „Nach Mitteilung des Deutschen Instituts für Vormundschaftswesen wird das Suchblattverfahren eingestellt. Die Einstellung des Suchblattes wird im letzten Suchblatt (Dezember 1984 oder Januar 1985) und in der Monatsschrift des Institutes „Der Amtsvormund" bekanntgemacht. Das Staatsministerium für Arbeit und Sozialordnung wird die bayerischen Jugendämter zu gegebener Zeit vorsorglich auf die Veröffentlichung hinweisen.

Ergänzend hat das Bayer. Staatsministerium für Arbeit und Sozialordnung mitgeteilt, daß es im Gegensatz zu der bisher vertretenen Auffassung nunmehr davon ausgeht, daß die Führung von Amtsvormundschaften, Amtspflegschaften und Amtsbeistandschaften dem Sozialleistungsbereich im Sinne des § 37 SGB I zuzurechnen ist.

Diese Rechtsauffassung wird von mir geteilt.

4.2. Telefonische Auskunft über Sozialdaten – an den Falschen

Ein (privater) Anrufer bei einer AOK hatte sich als Mitarbeiter einer anderen Sozialbehörde ausgegeben. Ein Bediensteter der AOK gab telefonisch über einen Versicherten Auskunft, und zwar über dessen Arbeitgeber sowie die Frage, ob der Betroffene zu einem bestimmten Zeitpunkt Mitglied der AOK war. Der Anrufer war ihm nicht bekannt.

Die mitgeteilten Angaben unterlagen dem Sozialgeheimnis gem. § 35 SGB I. Eine Offenbarungsbefugnis nach §§ 64 ff SGB war nicht gegeben, die Datenoffenbarung deshalb unzulässig. Sie war daher zu beanstanden. Die AOK machte in diesem Zusammenhang geltend, daß es sich um einen Einzelfall gehandelt habe, in dem entgegen der einschlägigen Dienstanweisung, abweichend von der bestehenden Übung, telefonisch Auskunft erteilt wurde, obwohl objektiv keine Gewißheit bestehen konnte, daß der Anrufer wirklich Mitarbeiter bei der auskunftsberechtigten Behörde war.

Dieser Einzelfall sei berichtet, da die telefonische Amtshilfe eine nützliche und weitverbreitete Art des Verwaltungsvollzuges ist, bei der aber dringend auf die gebotenen Vorsicht hingewiesen werden muß.

4.3. Übermittlung der Anschriften von Schulabgängern aus dem Melderegister an Krankenkassen

Aufgrund von Hinweisen habe ich erfahren, daß Krankenkassen Namenslisten aus Jahresberichten der Schulen, in denen zwar die Namen der Schüler, nicht aber die Wohnanschrift enthalten sind, Einwohnermeldeämtern mit der Bitte um Ergänzung der Wohnanschrift vorgelegt hätten. Ziel der Aktion war Aufklärung und Werbung von Mitgliedern für die Krankenkassen.

Den vom Bundesversicherungsamt (mit Rundschreiben vom 24.5.1983) den bundesunmittelbaren Krankenversicherungsträgern bekanntgegebenen sogenannten Wettbewerbsgrundsätzen ist zu entnehmen, daß Krankenkassen/

Ersatzkassen im Bereich der Aufklärung und Werbung am Wettbewerb teilnehmen und damit privaten Unternehmen gleichzustellen sind. Die Zulässigkeit einer Auskunft aus dem Melderegister richtet sich in diesem Fall daher grundsätzlich nach Art. 34 Abs. 1 MeldeG. Dabei wäre allerdings Vorsorge dafür zu tragen, daß nicht die speziellere Vorschrift des Art. 62 Abs. 2 EUG unterlaufen wird, die einer Schule die Herausgabe entsprechender Schülerdaten untersagt („falls nicht ein rechtlicher Anspruch auf die Herausgabe der Daten nachgewiesen" wäre, was hier nicht der Fall ist). Inzwischen stellt die Vollzugsbekanntmachung des Bayerischen Staatsministerium des Innern zum Bayerischen Meldegesetz (VollzBekMeldeG) vom 28.4.1984 (MABl. Nr. 10/84 S. 177) die Frage der Übermittlung von Schülerdaten zu Ergänzung von Daten aus einem Jahresbericht klar. Danach ist ein Mißbrauch des Sammelauskunftsverfahrens anzunehmen, wenn Namenslisten ohne weitere Adressenangaben (z.B. Mitgliederlisten von Verbänden, Jahrbücher, Jahresberichte der Schulen, Namenslisten von Behördenangehörigen) von der Meldebehörde durch die Anschrift ergänzt werden sollen (z.B. für Werbezwecke). In solchen Fällen ist die Sammelauskunft zu verweigern. Die Meldebehörden dürfen danach Auskunftsbegehren der vorbezeichneten Art zu Werbezwecken nicht mehr entsprechen.

4.4. Vorlage und Abgabe von Sozialhilfeakten an staatliche Archive

Von verschiedener Seite war ich um Äußerung zu der Frage gebeten worden, inwieweit Sozialhilfeakten und andere Sozialakten unter Beachtung der Vorschriften über das Sozialgeheimnis an das Staatsarchiv abgegeben werden können. Ich habe dazu die folgende Auffassung vertreten:

Die Vorlage von Sozialakten bei einem Staatsarchiv zur Prüfung auf archivwürdiges Archivgut und eine spätere Abgabe dieser Akten an das Staatsarchiv ist als Offenbarung von Angaben über persönliche und sachliche Verhältnisse der Empfänger von Sozialleistungen zu betrachten. Eine solche Offenbarung ist nach § 35 Abs. 2 SGB I nur unter den Voraussetzungen der §§ 67 – 77 SGB X zulässig. Nach keiner dieser Bestimmungen ist eine Offenbarung von Sozialdaten zu Archivzwecken vorgesehen. Ob der Gesetzgeber diese Fragestellung übersehen hat oder absichtlich nicht geregelt hat, muß dabei dahinstehen. Die Rechtslage hat zur Folge, daß Sozialakten, die lebende Personen betreffen, dem Staatsarchiv nur dann vorgelegt oder überlassen werden können, wenn entweder die Betroffenen in die Aktenweitergabe eingewilligt haben, oder die Sozialakten durch Löschung der Identifizierungsangaben so aufbereitet wären, daß die Betroffenen nicht mehr bestimmt werden können. Sofern Sozialleistungsempfänger oder die sonstigen Betroffenen verstorben sind, steht meines Erachtens Art. 35 SGB I einer Datenoffenbarung an das Staatsarchiv nicht entgegen. Obwohl eine ausdrückliche Regelung im SGB zu den Daten Verstorbener fehlt, ist wohl davon auszugehen, daß der Schutz der Sozialdaten entsprechend dem des Datenschutzgesetzes mit dem Tode des Betroffenen endet.

Ich habe daher angeregt, Sozialakten an das Staatsarchiv nur dann vorzulegen oder abzugeben, wenn die Betroffenen verstorben sind oder ihr Ableben mit hoher Wahrscheinlichkeit anzunehmen ist (Vollendung des 100. Lebensjahres). Zum Schutze der Persönlichkeitssphäre etwa noch lebender Angehöriger sollte zusätzlich für die Benutzung dieser Akten im Staatsarchiv eine Sperrfrist von etwa 30 Jahren eingehalten werden.

Schwieriger ist die Situation allerdings, wenn die Sozialakten – was häufig der Fall ist – medizinische Daten enthalten. Nach § 76 Abs. 1 SGB X ist der Sozialleistungsträger gehalten, solche Daten nur unter den Voraussetzungen zu offenbaren, unter denen die in § 203 Abs. 1 und 3 StGB genannten Personen selbst zur Offenbarung befugt wären. Nach § 203 Abs. 4 StGB ist die unbefugte Offenbarung fremder Geheimnisse auch nach dem Tode des Betroffenen strafbar. Auch in diesen Fällen wird die Befugnis zur Offenbarung nur vorliegen, wenn er eine ausdrückliche Zustimmung des Betroffenen – etwa ausgesprochen noch vor seinem Tode – oder seine mutmaßliche Einwilligung vorliegen oder aufgrund besonderer Gesetze oder eines Notstandes die Offenbarung erlaubt ist. Eine ausdrückliche gesetzliche Befugnis liegt wohl nicht vor. Diese könnte eventuell durch ein künftiges Archivgesetz geschaffen werden. Inwieweit die mutmaßliche Einwilligung des Betroffenen angenommen werden kann, erscheint zweifelhaft. Jedenfalls kann nicht das generelle Vorliegen einer mutmaßlichen Einwilligung unterstellt werden, um die vollständige Abgabe der Akten an das Staatsarchiv zu rechtfertigen, wenn medizinische Daten enthalten sind. Auch die Ausnahmeregelung des § 76 Abs. 2 SGB X über die Weitergabe von Gutachten und Bescheinigungen wegen der Erbringung von Sozialleistungen würden eine Abgabe an das Staatsarchiv nicht rechtfertigen, weil eine derartige Weitergabe nicht dem Vollzug einer gesetzlichen Aufgabe im Sinne des § 69 Abs. 1 Nr. 1 SGB X dienen würde.

Gleichwohl ließe sich die Frage der Abgabe von Aktenmengen, für deren Aufbewahrung beispielsweise nicht genügend Raum vorhanden ist, einstweilen lösen: Es bestehen keine datenschutzrechtlichen Bedenken dagegen, daß Sozialakten in den Räumen des Staatsarchivs lediglich für die Sozialbehörde eingelagert würden. Dabei wäre allerdings zu beachten, daß die abgebende Stelle in diesem Falle allein verfügungsberechtigt bleibt und weder das Personal des Archivs noch andere Personen oder Stellen – außer den obengenannten Fällen unter Annahme einer Befugnis – Zugang erhalten. Die zu treffende Auswahl archivwürdiger Akten könnte anhand allgemeiner Vorgaben des Staatsarchivs erfolgen. Durch besondere Schutzvorkehrungen technischer und organisatorischer Art in den Räumen des Staatsarchivs wäre sicherzustellen, daß auf die Sozialdaten nicht unberechtigt zugegriffen werden kann.

Es sei darauf hingewiesen, daß sich bei Unterlagen, die dem Steuergeheimnis unterliegen, dieselbe Problematik ergibt, klärende gesetzliche Regelungen erscheinen dringend geboten.

4.5. Datenverarbeitung durch Unternehmen im Auftrage ihrer Betriebskrankenkassen

Betriebskrankenkassen bedienen sich bei der Auszahlung von Leistungen teilweise des EDV-Service des Arbeitgebers. Von außerhalb Bayerns war ich darauf hingewiesen worden, daß in einem Falle zwischen Betriebskrankenkasse und einem Unternehmen eine Vereinbarung getroffen

wurde, nach der Barleistungen der Betriebskrankenkasse, die eine Lohnersatzfunktion haben (Kranken- und Mutterschaftsgeld sowie artgleiche Auftragsleistungen) durch den Betrieb an die Lohnempfänger mit dem Lohn bzw. anstelle des Lohns ausbezahlt werden. Dabei können Lohnüberzahlungen des Unternehmens mit den Barleistungen der BKK verrechnet werden, soweit sie für Zeiten geleistet wurden, für die Barleistungen der BKK gewährt werden. Vorschüsse auf Krankengeld würden vom Lohnbüro bezahlt und mit der nächsten Zahlung verrechnet. Nach Auffassung der zuständigen Aufsichtsbehörde konnte bei dieser Sachlage von einer Datenverarbeitung im Auftrag im Sinne von § 31 Abs. 1 Nr. 3 BDSG nicht gesprochen werden.

Auf meine Bitte hat der Landesverband der Betriebskrankenkassen in Bayern daher bei den Mitgliedskassen rückgefragt und festgestellt, daß in Bayern, soweit Betriebskrankenkassen sich zur Auszahlung von Barleistungen der EDV-Anlagen des Arbeitgebers bedienen, lediglich die Überweisung der von der Betriebskrankenkassen vorgegebenen Zahlbeträge auf das Lohn-/Gehaltskonto des Arbeitnehmers durchgeführt werden. Nach dem hierfür geltenden Mustervertrag zwischen Betriebskrankenkassen und Arbeitgeber (Auftragnehmer) verarbeitet letzterer personenbezogene Daten ausschließlich gemäß den Weisungen des Auftraggebers (BKK). Er verwendet die zur Datenverarbeitung überlassenen Daten nicht anderweitig und bewahrt sie nicht länger auf, als es der Auftraggeber bestimmt. Die von der vorgenannten Aufsichtsbehörde geäußerten Bedenken haben sich daher bisher bei bayerischen Betriebskrankenkassen nicht ergeben.

4.6. Darf eine Gemeinde Rentendaten speichern?

In einer Eingabe wurde Beschwerde darüber geführt, daß die kreisangehörige Gemeinde in jährlichen Abständen Daten über Rentenbezieher für eine Kartei aller in der Gemeinde wohnenden Rentner erhebe. Der Beschwerdeführer bat, sich vor allem für die Löschung der Höhe seiner Rente einzusetzen.

Meine Nachforschungen ergaben, daß die Gemeinde – wie wohl viele andere Gemeinden auch – ihre Bürger seit Jahren bei der Antragstellung für Renten nach der gesetzlichen Rentenversicherung unterstützt. Die Gemeinde führt eine sogenannte Rentenkartei, in der die wichtigsten Daten aus dem Rentenbescheid festgehalten werden, damit bei einem Verlust des Rentenbescheids Ausfertigungsdatum, Rentenzeichen usw. festgehalten sind. Außerdem kann die Gemeinde bei der Vorlage des Rentenbescheides Ratschläge im Bereich des Rentenrechts und hinsichtlich sonstiger Unterstützungsansprüche geben. Eine solche bürgerfreundliche Leistung der Gemeinde begrüße ich ausdrücklich. Als Rechtsgrundlage für die Tätigkeit kommt Art. 58 Abs. 2 der Bayerischen Gemeindeordnung in Betracht. Danach zählt es zu den Pflichten und Aufgaben der Gemeinde, in den Grenzen ihrer Verwaltungskraft den Gemeindeangehörigen bei der Einleitung von Verwaltungsverfahren behilflich zu sein, auch wenn für deren Durchführung eine andere Behörde zuständig ist. Das Sozialgesetzbuch enthält zum gleichen Sachverhalt in § 16 Abs 2 SGB I die Bestimmung, daß ein Sozialleistungsantrag als zu dem Zeitpunkt gestellt gilt, in dem er (u.a.) bei einer Gemeinde eingegangen ist. Weitere Aufgaben im Sozialleistungsbereich werden kreisangehörigen Gemeinden im Sozialgesetzbuch nicht zugewiesen. Die Erhebung von Daten über Bürger im Rahmen dieser Hilfestellung erfolgt auf freiwilliger Basis. Die Betroffenen sind daher nach Art. 16 Abs. 2 BayDSG deutlich auf die Freiwilligkeit ihrer Angaben hinzuweisen. Aus dem gleichen Grund darf die von der Gemeinde an die betreffenden Bürger gerichtete Information über diese Hilfeleistung und die Aufforderung zur Angabe von personenbezogenen Daten für die Kartei der Gemeinde keinesfalls als „Ladung" der Rentenempfänger formuliert werden. Der Dienstleistungscharakter und die Freiwilligkeit der Inanspruchnahme würden sonst nicht deutlich.

Die Gemeinde hat aufgrund des mit ihr geführten Schriftwechsels ein neues (Standard-)Anschreiben an die Rentenempfänger formuliert, in dem die Funktion der Rentenkartei und die Freiwilligkeit der Inanspruchnahme dieser Hilfe sowie der Angabe personenbezogener Daten hinreichend deutlich erläutert wird. Die Gemeinde hat außerdem darauf verzichtet, die jeweilige Rentenhöhe lückenlos fortlaufend zu erfassen und in der Kartei fortzuschreiben. Sie hat festgestellt, daß für die oben geschilderte Nachweisfunktion der Kartei die einmalige Vorlage des Rentenbescheids nach der Bescheiderteilung genügt.

4.7. Auftragsdatenverarbeitung – auftragswidrige Datennutzung durch den Auftragnehmer

Durch die Eingabe eines Apothekers wurde ich darauf aufmerksam, daß eine (privatrechtliche) Verrechnungsstelle für Apotheken möglicherweise personenbezogene Daten, die sie zur Abwicklung von Datenverarbeitung im Auftrag von Verbänden der gesetzlichen Krankenkassen erhalten hatte, auch für andere eigene Zwecke verwendet haben könnte. Da das Schwergewicht in der datenschutzrechtlichen Problematik hier im Bereich nichtöffentlicher Stellen liegt, habe ich die Eingabe an die zuständige bayerische Bezirksregierung als Datenschutzaufsichtsbehörde für den nichtöffentlichen Bereich weitergeleitet. Gleichzeitig habe ich mich jedoch an die bayerischen Krankenkassenverbände gewandt, damit von seiten der öffentlichen Stellen, die meiner Datenschutzkontrolle unterliegen und die in diesem Falle die Auftraggeber sind, auf die Datenverarbeitung bei deren Auftragnehmer eingewirkt werde. Ich habe angeregt, die zwischen der Abrechnungsstelle und den Krankenkassenverbänden geschlossene Vereinbarung auf der Grundlage von § 80 SGB X, der nähere Vorschriften über die Auftragsdatenverarbeitung bei Sozialdaten enthält, zu überprüfen und insbesondere der Vorschrift des § 80 Abs. 2 SGB X anzupassen, sowie gegenüber der Abrechnungsstelle als Auftragnehmer klarzustellen, daß eine Verwendung der überlassenen Daten nach § 80 Abs. 4 SGB X für eigene Zwecke der Abrechnungsstelle unzulässig ist. Daraufhin wurde mir eine protokollarische Erklärung übersandt, nach der die Landesverbände der gesetzlichen Krankenkassen in Bayern mit der Verrechnungsstelle erneut vereinbarten, daß die überlassenen Daten entsprechend § 80 Abs. 4 SGB X nicht anderweitig gebraucht werden dürfen bzw. eine Verwendung für eigene Zwecke des Auftragnehmers unzulässig ist. Die Datenschutzaufsichtsbehörde hat die Verhaltensweise der Verrechnungsstelle beanstandet.

Der Fall gibt Anlaß, auf die Vorschrift des § 80 Abs. 2 SGB X besonders hinzuweisen. Danach darf ein Auftrag zur Datenverarbeitung überhaupt nur erteilt werden, wenn der Datenschutz beim Auftragnehmer den Anforderungen genügt, die für den Auftraggeber gelten. Der Auftraggeber ist verpflichtet, erforderlichenfalls Weisungen zur Ergänzung von Datensicherungsmaßnahmen zu erteilen. Für wesentlich halte ich aber, daß nach Satz 3 der genannten Vorschrift bei einem privatrechtlich organisierten Auftragnehmer – wie im vorliegenden Fall – die Auftragserteilung außerdem voraussetzt, daß sich der Auftragnehmer schriftlich damit einverstanden erklärt hat, daß der Auftraggeber jederzeit berechtigt ist, mit den in § 30 Abs. 2 und 3 des BDSG genannten Mitteln die Einhaltung der Vorschriften über den Datenschutz unter ergänzenden Weisungen nach Satz 2 zu überwachen. Der Auftragnehmer hat sich also einer Datenschutzkontrolle des Auftraggebers zu unterwerfen. Eine entsprechende Unterwerfungserklärung wurde nach Mitteilung des Landesverbands der Ortskrankenkassen inzwischen abgegeben.

Der Fall ist außerdem berichtenswert, weil er erneut belegt, daß größere Datensammlungen auch bei Auftragnehmern immer wieder einem erheblichen Druck auf Zulassung weiterer Nutzungen als ursprünglich vorgesehen ausgesetzt sind (siehe auch meine Ausführungen zur „Anziehungskraft größerer Datensammlungen" im 5. Tätigkeitsbericht Textziffer 1.1 Seite 4 ff).

4.8. Umfang der Datenerhebung beim Antrag auf Sozialhilfe

Über Inhalt und Form von Antragsformularen für Sozialhilfe sind mehrfach Beschwerden eingegangen. So wurde wiederholt moniert, daß unverhältnismäßige oder überflüssige Angaben gefordert würden, die nicht in Zusammenhang mit der Hilfegewährung ständen. In einer Eingabe wurde direkt auf Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil Bezug genommen, nach denen sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen. Die kritisierten Fragestellungen betrafen wiederum die Frage nach dem schuldigen Teil einer Ehescheidung, die Verwendung des Begriffs „uneheliche" Kinder, die Frage nach dem Grund einer Arbeitslosigkeit, die Verpflichtung vorübergehende Abwesenheit, Krankenhausaufenthalte usw. auch von Haushaltsangehörigen unverzüglich und unaufgefordert dem Träger der Hilfe mitzuteilen, pauschale Ermächtigungen zu Nachfragen bei allen Geldinstituten, bei allen Ärzten, Kliniken etc. anstatt konkretisierter Ermächtigungen für den bestimmten einzelnen Fall, die Forderung nach einer Generalermächtigung zur Einsicht in Gerichts- und sonstige Akten, sowie die Frage nach der Konfession. Bei dieser Gelegenheit wurde auch die Verletzung von Persönlichkeitsrechten bei Behinderten durch den Sprachgebrauch von Fragebögen moniert wie etwa bei der Frage, seit wann jemand seinen jetzigen Wohnort „zugewiesen" oder „umgesiedelt" worden sei, oder die Verpflichtung, sich vorgeschlagenen Maßnahmen bzw. evtl. Anstaltsaufnahme zu unterziehen und sie auch „ordnungsgemäß durchzuführen", was angesichts des freiwilligen Charakters der Inanspruchnahme von Sozialhilfe unangemessen sei.

Einzelnen Beschwerden, die bei mir eingingen, bin ich jeweils nachgegangen und habe gegebenenfalls den jeweiligen Träger der Sozialhilfe um Änderung der verwendeten Formblätter gebeten. Wegen der Vielzahl der verschiedenen Sozialhilfeanträge ist jedoch eine Überprüfung aller verwendeten Formblätter nicht möglich. Ich habe daher beim Landkreisverband Bayern, beim Verband der Bayerischen Bezirke e.V. und beim Bayerischen Städtetag angeregt, unter Berücksichtigung der Bestimmungen des Bundesdatenschutzgesetzes und der vom Bundesverfassungsgericht im Urteil über das Volkszählungsgesetz entwickelten Grundsätze einen Musterentwurf für einen Sozialhilfeantrag zu erarbeiten und untereinander abzustimmen. Der Landkreisverband Bayern und der Bayerische Städtetag haben zugesagt, sich im Laufe des Jahres 1985 mit dem Thema „Musteranträge für Sozialhilfe" zu befassen.

4.9. Sozialbericht Suchtkranke

Zur Problematik der Datenerhebung u.a. für Rentenversicherungsträger mit Hilfe eines Formulares „Sozialbericht Suchtkranke" habe ich im zweiten und im vierten Tätigkeitsbericht Ausführungen gemacht (II, Seite 22 Nr. 4.1.4.3 und IV Seite 31/32 Nr. 3.4.6).

Seit dem Jahre 1979 wurde zwischen den Datenschutzbeauftragten des Bundes und der Länder und dem Verband Deutscher Rentenversicherungsträger (VDR) Form, Inhalt und Umfang der im Zusammenhang mit Rehabilitationsmaßnahmen nach § 1236 RVO verwendeten Sozialberichte bei Abhängigkeitskranken erörtert. Die bisher letzte Stellungnahme des VDR aus dem Berichtsjahr läßt erkennen, daß eine Annäherung der Standpunkte über den Umfang der Mitwirkungspflicht eines Abhängigkeitskranken bei der Erstellung des Suchtberichts nur in beschränktem Umfang erreicht werden konnte.

Gleichwohl halte ich an meiner Auffassung fest, daß in vielen Fällen eine vollständige Beantwortung der im Sozialbericht gestellten Fragen den Rahmen der Erforderlichkeit und damit der Mitwirkungspflicht der Leistungsberechtigten sprengt. Wegen der besonderen Schutzbedürftigkeit der im Sozialbericht erhobenen Daten ist eine Prüfung der Erforderlichkeit im Einzelfall vorzunehmen. Erforderlich ist meines Ermessens die Beantwortung der einzelnen Fragen nur, wenn ohne Kenntnis der Angaben Entscheidungen über

- die Zuständigkeit für die Leistungsgewährung,
- die Erfolgsaussichten der Suchtbehandlung,
- der Zeitpunkt des Therapiebeginns,
- die Auswahl der Behandlungsstätte und
- die Auswahl der Leistungen zur Rehabilitation in dem in den §§ 1237 – 1237b RVO bestimmten Umfang

nicht getroffen werden können. Die Forderung des VDR, wonach der Sozialarbeiter den Fragebogen immer vollständig auszufüllen habe, geht über dieses Ziel hinaus.

Meine Auffassung findet Unterstützung auch in den Grundsätzen, die das Bundesverfassungsgericht im Urteil zum Volkszählungsgesetz 1983 vertreten hat. Das Gericht führt u.a. aus: „Schon bislang ist anerkannt, daß die zwangsweise Erhebung personenbezogener Daten nicht

unbeschränkt statthaft ist, namentlich dann, wenn solche Daten für den Verwaltungsvollzug (etwa bei der Besteuerung oder für Gewährung von Sozialleistungen) verwendet werden sollen. Wie weit das Recht auf informationelle Selbstbestimmung und im Zusammenhang damit der Grundsatz zur Verhältnismäßigkeit sowie die Pflicht zu verfahrensrechtlichen Vorkehrungen (den Gesetzgeber) zu diesen Regelungen von Verfassungs wegen zwingen, hängt von Art, Umfang und denkbaren Verwendungen der erhobenen Daten sowie der Gefahr ihres Mißbrauchs ab. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen".

Diese Grundsätze wurden vom Bundesverfassungsgericht zwar in Zusammenhang mit der zwangsweisen Erhebung von Daten aufgestellt. Ich vertrete jedoch die Auffassung, daß das Argument der „Freiwilligkeit" bei der Abgabe des Sozialberichts nicht erfolgreich entgegengehalten werden kann, da aus der Sicht des Betroffenen ein faktischer Zwang besteht. Die Angaben eines Abhängigkeitskranken über seine soziale und gesundheitliche Situation zähle ich zu den schutzbedürftigsten persönlichen Daten überhaupt. Das Verhältnismäßigkeitsgebot wird daher zu engen Grenzen der Mitwirkungspflicht des Betroffenen führen. Diese Grenzen hat auch der Sozialarbeiter zu beachten, der den Sozialbericht erstellt. Die Mitwirkungspflicht von Antragsteller und Sozialarbeiter darf daher meines Erachtens nicht etwa dadurch aufgehoben werden, daß der Rentenversicherungsträger die vollständige Ausfüllung des Fragebogens verlangt und andernfalls den Antrag ohne nähere Prüfung zurückweist.

Von dieser Auffassung habe ich das Bayerische Staatsministerium für Arbeit und Sozialordnung, das Landesprüfungsamt für Sozialversicherung und die Bayerischen Landesversicherungsanstalten verständigt und darauf hingewiesen, daß ich eingehende Beschwerden anhand der genannten Kriterien prüfen werde.

4.10. Geschützte Sozialdaten – auf Krankenscheinen ohne Schutz

Die sogenannte „Vordruckvereinbarung", die zwischen der Kassenärztlichen Bundesvereinigung und den Bundesverbänden der gesetzlichen Krankenkassen geschlossen wurde, sieht für Krankenscheine, Überweisungsscheine, Arzneimittelverordnungsblätter und andere Vordrucke die Angabe des Arbeitgebers vor. Hiergegen haben sich in Anfragen bei meiner Geschäftsstelle freiwillige Mitglieder einer gesetzlichen Krankenkasse gewandt, die ihr Unverständnis über die Notwendigkeit einer Erhebung des Arbeitgebers äußerten. Das gleiche gilt für Versicherte, die gegenwärtig arbeitslos sind. Die Angabe des Arbeitgebers erzeugt namentlich bei Arbeitslosen ein Problem, das ein Petent in einem Brief an den Niedersächsischen Datenschutzbeauftragten plastisch dargestellt hatte: „Ich habe das selbst einmal durchgemacht und war erstaunt, wer alles mich daraufhin ansprach, teils mitleidig, teils schadenfroh: Sprechstundenhilfe beim Hausarzt, Hausarzt, Apothekenangestellte, Apotheker, Masseur, Taxifahrer bei Krankenfahrt, Krankenhausaufnahme, Schule durch ärztliche Bescheinigung für Fehlen. Man könnte ebensogut ein Inserat in die örtliche Zeitung setzen: „Ich bin arbeitslos."

Rechtlich ist der hier bestehende faktische Zwang, den Arbeitgeber oder die Tatsache der Arbeitslosigkeit Dritten gegenüber zu offenbaren, problematisch, da solche Angaben nach dem Sozialgesetz grundsätzlich geheimzuhalten sind und nur unter bestimmten gesetzlich festgelegten Voraussetzungen offenbart werden dürfen (§ 35 SGB I). Wenn der Betroffene jedoch durch die Verwendung der vorgeschriebenen Formulare gezwungen wird, zahlreichen Außenstehenden insbesondere seine Arbeitslosigkeit bekannt zu geben, wird dies dem geschilderten Anliegen des Sozialgesetzbuches nicht gerecht. Darüber hinaus halten nach meinen bisherigen Erkenntnissen Krankenkassen eine solche Angabe durchaus nicht durchwegs für erforderlich. Verschiedene gesetzliche Krankenkassen legen auf die Angabe des Arbeitgebers keinen Wert, andere halten die Angabe als „zusätzliches Kriterium" für die Prüfung der Mitgliedschaft oder der Kassenzuständigkeit für geeignet.

Ich habe meine Bedenken dem Landesverband der Ortskrankenkassen in Bayern vorgetragen. Dieser ist zwar für die Formulargestaltung nicht unmittelbar verantwortlich, zählt jedoch als Mitglied des Bundesverbandes der Ortskrankenkassen zu den Vertragspartnern der Vordruckvereinbarung. Der Landesverband hat sich der Empfehlung, die Partner der Vordruckvereinbarung mögen die Vordrucke – soweit kritisiert – ändern, angeschlossen und die Partner der Vordruckvereinbarung auf Bundesebene darüber unterrichtet. Die Beratungen dauern derzeit noch an. Es besteht daher Hoffnung, daß die Notwendigkeit, den Arbeitgeber bzw. die Tatsache der Arbeitslosigkeit auf Krankenscheinen Dritten zu offenbaren, demnächst entfällt.

4.11. Datenerhebung aus Anlaß eines „mißglückten Arbeitsversuches"

Wie im 6. Tätigkeitsbericht dargelegt, erheben gesetzliche Krankenkassen in Fällen eines „mißglückten Arbeitsversuches" personenbezogene Angaben. Sie dienen der Prüfung, ob ein versicherungspflichtiges Beschäftigungsverhältnis verliegt (6. TB, Tz. 4.11.2 Seite 65/66). Für problematisch war aus der Sicht des Datenschutzes erachtet worden, daß u.a. auch die Arbeitgeber mit einem Fragebogen über u.a. gesundheitliche Verhältnisse des Betroffenen befragt wurden. Inzwischen haben die Bemühungen der Datenschutzbeauftragten zu einem Verzicht der Krankenkassenverbände auf die Befragung des Arbeitgebers geführt. In Zweifelsfällen soll nur noch der behandelnde Arzt befragt werden.

4.12. Schutz von Daten, die einem Arzt anvertraut wurden, der vom Sozialleistungsträger beschäftigt wird

In meinem 5. Tätigkeitsbericht habe ich auf Auslegungschwierigkeiten hingewiesen, die sich bei der Anwendung des § 76 Abs. 1 SGB X ergeben hatten. Es war nämlich strittig gewesen, ob die durch die genannte Vorschrift beschränkte Weitergabe medizinischer Daten nur dann gilt, wenn die Daten dem Sozialleistungsträger von einem Arzt zugängig gemacht worden sind, der Nichtbeschäftigter des Sozialleistungsträgers sei. Demgegenüber hatte ich die Ansicht vertreten, daß auch Daten, die einem Arzt des Sozialleistungsträgers anvertraut wurden, einen gleich

starken Schutz genießen müssen. Nach Erlaß des Volkszählungsurteils des Bundesverfassungsgerichts sehe ich mich in dieser Ansicht bestärkt. Das Gericht führt dort u.a. aus, daß eine Einschränkung des Rechts auf informationelle Selbstbestimmung – zu der auch die Freiheit des Betroffenen zur Entscheidung über die Weitergabe seiner Daten zählt – nur im überwiegenden Allgemeininteresse zulässig ist und einer gesetzlichen Grundlage bedarf, die den Grundsätzen der Normenklarheit und Verhältnismäßigkeit genügen muß. Die Tatsache unterschiedlicher Rechtsauffassungen zur Anwendung des § 76 Abs. 1 SGB X könnte daher darauf hindeuten, daß die geforderte Normenklarheit fehlt. Um gleichwohl eine verfassungskonforme Anwendung sicherzustellen, müßte die den Betroffenen begünstigende Auslegung der Vorschrift gewählt werden und das bedeutet, daß im konkreten Fall § 76 Abs. 1 SGB X auch für Daten Anwendung zu finden hätte, die von bediensteten Ärzten der Versorgungsverwaltung zugänglich gemacht worden sind. § 76 Abs. 2 SGB X bleibt davon unberührt. Die Problematik wurde mit dem Bayerischen Staatsministerium für Arbeit und Sozialordnung erörtet. Es hat mir kürzlich mitgeteilt, daß zwischenzeitlich das Landesversorgungsamt Bayern angewiesen worden sei, meiner Auffassung in der geschilderten Rechtsfrage Rechnung zu tragen. Das Landesversorgungsamt Bayern hat mit Rundschreiben Nr. 1245/II vom 26.3.1985 sein früheres Rundschreiben vom 3.6.1982 nunmehr durch Einfügung der folgenden Formulierung geändert: „Dabei ist es hinsichtlich **medizinischer** Daten ohne Belang, ob die Daten dem Leistungsträger von einem behandelnden Arzt des Patienten oder durch eigene bedienstete Ärzte zugänglich gemacht worden sind. § 76 Abs. 1 findet also auf **alle** medizinischen Daten Anwendung, die dem Leistungsträger bekannt werden." Ich begrüße diese Klarstellung.

4.13. Welche medizinischen Daten darf eine Krankenkasse einem anderen Sozialleistungsträger offenbaren? (Umfang der Ausnahmeregelung nach § 76 Abs. 2 SGB X)

Zur Weitergabe von Daten über gesundheitliche Verhältnisse zwischen Sozialleistungsträgern – die gewissen Beschränkungen nach § 76 Abs. 2 SGB X unterliegt – habe ich im 6. Tätigkeitsbericht unter Nr. 4.11.4, Seite 66/67 ausführlich Stellung genommen. Im Berichtsjahr hatte mich nun eine Allgemeine Ortskrankenkasse um Stellungnahme zu der Frage gebeten, ob auf Anfrage von Berufsgenossenschaften diesen alle Krankheitsdaten des Versicherten offenbart werden müssen. Eine Berufsgenossenschaft forderte beispielsweise unabhängig vom Eintritt des schädigenden Ereignisses und ohne Rücksicht auf Krankheiten, die niemals eine Ursache für eine Unfallschädigung oder eine Berufskrankheit sein können, die Offenbarung sämtlicher medizinischer Angaben. Die AOK wollte nun klären, ob eine Übersendung des vollständigen Inhalts der Leistungskarte durch § 69 SGB X abgedeckt sei. Hierzu habe ich folgende Ansicht vertreten:

Nach § 69 Abs. 1 Nr. 1 SGB X ist eine Offenbarung personenbezogener Daten zulässig, soweit sie erforderlich ist für die Erfüllung einer gesetzlichen Aufgabe nach dem SGB durch eine in § 35 SGB I genannte Stelle. Es ist daher zu prüfen, ob regelmäßig alle auf der Leistungskarte eines Versicherten verzeichneten Angaben vom Träger der Unfallversicherung benötigt werden und damit die Bekanntgabe dieser Daten als „erforderlich" im Sinne der genannten Bestimmung anzusehen ist.

Die Vielfalt der Fallgestaltungen ermöglicht keine allgemeine Aussage über den Umfang der zulässigen Offenbarungen zur Erfüllung der gesetzlichen Aufgaben der Unfallversichungsträger. Nicht selten dürfte es aber in den oft über viele Jahre geführten Unterlagen der gesetzlichen Krankenkassen in sich abgeschlossene Vorgänge geben, die der Unfallversicherungsträger zu seiner Aufgabenerfüllung nicht kennen muß. Zu denken ist hier insbesondere an Vorerkrankungen, die ohne Nachwirkungen verlaufen sind und keinerlei Bezug zu dem Gesundheitszustand haben, für den nurmehr eine Leistung nach dem Recht der Unfallversicherung erbracht werden soll. Das gleiche gilt für Vorgänge, die wegen der Länge der zurückliegenden Zeit keine Bedeutung für die gegenwärtige Leistungsgewährung haben. In solchen Fällen wird die Weitergabe von Krankheitsdaten von den Betroffenen als besonders einschneidend empfunden werden, vor allem, wenn die Gesundheitsstörungen einen Bereich betreffen, die auch heute noch häufig der gesellschaftlichen Ächtung unterliegen (z.B. psychische Störungen, Geschlechtskrankheiten u.ä.).

Andererseits wird in bestimmten Fällen – insbesondere wenn die Vorerkrankungen eine Beurteilung des ursächlichen Zusammenhangs des gegenwärtigen Krankheitsbildes mit der beruflichen Tätigkeit ermöglichen – die Kenntnis der bei der gesetzlichen Krankenkasse vorhandenen Unterlagen für die Leistungserbringung im Bereich der Unfallversicherung erforderlich im Sinne des § 69 Abs. 1 Nr. 1 SGB X sein.

Ein gesetzeskonformer Vollzug dieser Bestimmung führt somit im Ergebnis dazu, daß vor einer Offenbarung an den Träger der Unfallversicherung von der gesetzlichen Krankenkasse eine grobe Überprüfung der Angaben auf der Leistungskarte (bzw. in den sonstigen Unterlagen) unter dem Gesichtspunkt der Erforderlichkeit durchzuführen ist und nur solche Informationen weitergegeben werden dürfen, für die diese Bedingung zutrifft. Dies setzt eine entsprechende kurze Darlegung des Anlasses für die Datenanforderung durch den Träger der Unfallversicherung voraus.

Ich verkenne nicht, daß eine solches Verfahren mit einer zusätzlichen arbeitsmäßigen Belastung vor allem der datenabgebenden Stelle verbunden ist. Im Hinblick auf den Grundsatz der Verhältnismäßigkeit des Verwaltungshandelns muß dies aber wohl in Kauf genommen werden, da auch der Offenbarung von Krankheitsdaten die Qualität einer Einschränkung des Grundrechts auf informationelle Selbstbestimmung grundsätzlich zukommt. Medizinische Befunde und andere Patientendaten sind deshalb im Rahmen der beruflichen Schweigepflichten nach § 203 SGB besonders geschützt. Wenn auch § 76 Abs. 2 SGB X einer Offenbarung solcher Daten im Zusammenhang mit § 69 Abs. 1 Nr. 1 SGB X erleichtert, besteht doch gerade hier die Gefahr, daß durch eine nicht erforderliche Offenbarung das geschützte Persönlichkeitsrecht des Betroffenen unverhältnismäßig und damit unzulässig beeinträchtigt wird. Darüber hinaus ist zu berücksichtigen, daß der Umfang der Ausnahmeregelung nach § 76 Abs. 2 SGB X eng begrenzt ist. Ich weise in diesen Zusammenhang auf meine Ausführungen im 5. Tätigkeitsbericht hin (siehe oben). Bei

der Erfüllung seiner Aufgabe wird der Träger der Unfallversicherung den erheblichen Sachverhalt in erster Linie im Rahmen der Mitwirkung beim Antragsteller bzw. Leistungsempfänger selbst zu ermitteln haben (vergl. auch § 60 ff SGB I). Nimmt ein Antragsteller im Rahmen seiner Mitwirkungspflicht selbst Bezug auf Vorgänge, die in den Unterlagen der gesetzlichen Krankenkasse gespeichert sind, so habe ich keine Bedenken, entsprechende Angabe an den Unfallversicherungsträger zu offenbaren. Außerdem mag in einzelnen Fällen die Einholung einer Einwilligung zur Datenoffenbarung nach § 67 SGB X praktische Probleme beim Vollzug überwinden helfen. Dabei sind jedoch die Grenzen der Mitwirkungspflichten nach § 65 SGB I zu beachten.

Die von mir unterrichteten Landesverbände der gesetzlichen Krankenkassen in Bayern haben sich meine Auffassung zu eigen gemacht und die Mitgliedskassen davon unterrichtet. Der Hauptverband der gewerblichen Berufsgenossenschaften e.V. in Bonn wurde durch den Bundesbeauftragten für den Datenschutz unterrichtet.

4.14. Überprüfung von Datenerhebung und Speicherung durch die Landesstiftung „Hilfe für Mutter und Kind"

Aufgrund einer Eingabe hatte ich die Erhebung und Speicherung von Daten durch die Landesstiftung „Hilfe für Mutter und Kind" zu überprüfen. Die rechtsfähige staatlich verwaltete Stiftung des öffentlichen Rechts hat den Zweck, Hilfen für Schwangere in Notlagen zu gewähren (§ 2 Abs. 1 Nr. 1 der Satzung). Sie darf niemanden durch Ausgaben, die dem Zweck der Stiftung fremd sind, oder durch unverhältnismäßig hohe Unterstützungen, Zuwendungen oder Vergünstigungen begünstigen. Mittel dürfen nur für satzungsgemäße Zwecke verwendet werden. Der Förderungsbereich ist durch vom Stiftungsrat beschlossene Vergabegrundsätze näher abgegrenzt. Über das Verfahren der Leistungsgewährung kann die Stiftung im Rahmen der geltenden Vorschriften selbst entscheiden. Sie kann sich die Entscheidung über die Leistungsgewährung entweder selbst vorbehalten oder sich anderer Stellen, z.B. staatlich anerkannter Beratungsstellen für Schwangerschaftsfragen bedienen.

Hält die Landesstiftung aufgrund ihrer Erfahrungen bei der Vergabepraxis die Vorlage der Antragsunterlagen auch dann für erforderlich, wenn die Leistungsgewährung mit Hilfe der Beratungsstellen erfolgt, vermag ich dies wegen der erwähnten Organisationshoheit datenschutzrechtlich nicht zu beanstanden. Ich habe jedoch angeregt, die Hilfegesuche nebst Belegen nach Prüfung durch die Landesstiftung urschriftlich an die Beratungsstellen zurückzusenden und nur die notwendigsten personenbezogenen Daten bei der Stiftung vorzuhalten. Die Stiftung ist zum Speichern der erforderlichen personenbezogenen Daten der Hilfesuchenden berechtigt, da ihr die Vergabe von Mitteln durch die Satzung als aufgabenzuweisende Rechtsnorm aufgegeben wird (Art. 6 Abs. 1 BayDSG). Von Schwangeren dürfen jedoch nur Einzelangaben über persönliche und wirtschaftliche Verhältnisse verlangt werden, die zur Feststellung der Leistungsvoraussetzungen und zur Bearbeitung des Hilfeersuchen erforderlich sind. Die Antragsformulare wurden diesen Anforderungen angepaßt. Die Hilfesuchende hat im Zusammenhang mit der Prüfung der Anspruchsvoraussetzungen in zumutbarem Umfang eine Pflicht zur Mitwirkung bei der Sachaufklärung. Die im nunmehr verwendeten Antragsformular verlangte Einverständniserklärung, wonach die zur Bearbeitung des Hilfegesuchs erforderlichen Erkundigungen bei der zuständigen Sozialhilfeverwaltung eingeholt werden können, erscheint mir nicht unverhältnismäßig.

Bei der Prüfung der Verschwiegenheitspflichten nach Art. 8 Schwangerenberatungsgesetz ist zu berücksichtigen, daß eine staatlich anerkannte Beratungsstelle hier in zwei verschiedenen getrennt zu sehenden Funktionen tätig wird. Zum einen wird die Beratungsstelle im „eigentlichen" Bereich, der Beratung nach § 218 StGB, tätig, der auch durch die strafrechtliche Sanktion des § 203 Abs. 1 Nr. 4 a StGB umfaßt ist. Auf diese Funktion bezieht sich der zuvor erwähnte Art. 8 des Schwangerenberatungsgesetzes. Der zweite Aufgabenbereich, die Vermittlung von praktischen Hilfen, ist in Art. 5 Abs. 1 Schwangerenberatungsgesetz geregelt. Durch die Formulierung „über die Beratung hinaus" ist klargestellt, daß es sich bei der Bewilligung von Leistungen der Landesstiftung um einen von der Beratung unabhängigen Bereich handelt und insoweit Art. 8 Schwangerenberatungsgesetz nicht unmittelbar Anwendung findet. Da Beratung und praktische Hilfe in vielen Fällen jedoch nicht voneinander zu trennen sind, habe ich empfohlen, im Hilfeantrag eine entsprechende Einwilligungserklärung der Hilfesuchenden aufzunehmen.

Die Stiftung ist meinen Anregungen gefolgt.

4.15. Krankengeschichten in Sozialakten?

Krankenhäuser melden im Rahmen des § 121 Bundessozialhilfegesetz bei der Geltendmachung von Eilfällen die Krankheitsdiagnose an den Sozialhilfeträger. In bestimmten Fällen können sich deswegen besonders sensible Daten – beispielsweise über Erkrankungen oder Behandlungen, die normalerweise Dritten gegenüber geheimgehalten werden, weil sie als diskriminierend gelten, in Sozialakten finden bzw. ansammeln. Ich habe daher den Verband der Bayerischen Bezirke um Erläuterung für die Notwendigkeit der Angabe der aktuellen Krankheitsdiagnose gebeten. Von dort wurde geltend gemacht, daß die Einweisungsdiagnose erforderlich sei zur Feststellung des Eilfalls nach § 121 BSHG, zur Zuordnung der Hilfeart, zur Feststellung, welcher Sozialhilfeträger sachlich zuständig ist, zur Feststellung vorrangiger Ansprüche, z.B. eines Rentenversicherungsträgers bei Tbc-Verdacht oder eines Schadensersatzpflichtigen bei einem Unfall, zur Feststellung nachgehender Ansprüche nach § 183 RVO und bei einem Ausländer zur Feststellung des Anspruchs nach § 120 BSHG.

Der Verband hat jedoch mitgeteilt, die Bezirke würden darauf achten, daß die genannten medizinischen Unterlagen gesondert von den übrigen Aktenunterlagen geführt werden. Dies ist aus der Sicht des Datenschutzes zu begrüßen, da dadurch die Vernichtung dieser Unterlagen, soweit sie für die Leistungsgewährung nicht mehr erforderlich sind, erleichtert wird. Vereinfacht wird mit einer solchen Vorgehensweise auch die Trennung der erforderlichen/nichterforderlichen Aktenteile bei einer im übrigen zulässigen Aktenübersendung an andere Sozialbehörden und Gerichte.

5. Polizei

5.1. Zur Lage des Datenschutzes

Rückblickend auf die letzten 12 Monate meine ich feststellen zu können, daß auch im Sicherheitsbereich der Datenschutz in Bayern zunehmend zur Selbstverständlichkeit wird. Natürlich hat es auch in Bayern eine Reihe von Datenschutzproblemen gegeben, habe ich bei Prüfungen Fehler festgestellt, gibt es hin und wieder Ablehnung gegen den Datenschutz. Doch glaube ich, sollte man dies im Hinblick auf die Gesamttendenz nicht überbewerten. In diesem Zusammenhang habe ich mich auch über die Kriminalstatistik in Bayern für das Jahr 1984 gefreut. Danach hat die Polizei 1,7% weniger Straftaten registriert, in der Landeshauptstadt München betrug die Abnahme sogar 2,7%. Fast 60% der Fälle konnte die Polizei aufklären. Diese Zahlen sind meines Erachtens auch ein Beweis dafür, daß der Datenschutz entgegen anderslautender Behauptung die Arbeit der Polizei nicht wirklich beeinträchtigt.

Gerade bei der Polizei versuche ich besonders um Verständnis für die Belange des Datenschutzes zu werben. Dies geschieht zum einen durch zahlreiche Vorträge vor Polizeibeamten. Aber auch bei Prüfungen, die ich in den letzten 12 Monaten in gesteigerter Zahl durchgeführt habe, bin ich nicht in erster Linie bestrebt, Beanstandungen auszusprechen. Auch sehe ich nicht allein in einer möglichst großen Zahl von gelöschten Daten und vernichteten Akten schon einen Erfolg für den Datenschutz. Wichtig erscheinen mir gerade bei Prüfungen die Erörterungen der Probleme und ein zum Teil gemeinsames Suchen nach Lösungen zu sein. Denn es dürfte unbestritten sein, daß im Einzelfall eine Abwägung zwischen polizeilichen Interessen und berechtigten Belangen der Bürger schwierig sein kann. Doch wo sind im juristischen Bereich Abwägungen nicht manchmal schwierig, wenn unterschiedliche Rechtsinteressen aufeinanderstoßen?

Um so mehr bedauere ich, daß in einzelnen Fachzeitschriften der Polizei und in Verbandsblättern zum Teil recht unsachlich über den Datenschutz berichtet wird. Manche dieser Beiträge sind geradezu polemisch. Sie schüren unnötigerweise Emotionen bei der Polizei gegen den Datenschutz und können somit eine Zusammenarbeit erschweren.

In diesem Zusammenhang bedauere ich es auch, daß insbesondere ein polizeilicher Berufsverband ein gespanntes Verhältnis zum Datenschutz in seinen Publikationen zeigt. So kann ich auch einem Satz zum Datenschutz im Beschluß seines Delegiertentages „Dateien der Strafverfolgungsbehörden sind nach den Erfordernissen vitaler Gemeinschaftsinteressen und nicht nach den Individualinteressen auszurichten" nicht beipflichten. Hier wird verkannt, daß das Bundesverfassungsgericht nicht erst in seiner Entscheidung zum Volkszählungsgesetz 1983 eine Abwägung zwischen den Interessen des Individuums und denen der Gemeinschaft verlangt. Wenn in einem solchen Zusammenhang dann noch behauptet wird, daß eine solche Aussage auf den „Erfahrungen praktizierender Kriminalisten in den letzten Jahren" beruhe, stimmt mich dies besonders nachdenklich. Denn bei meinen vielfachen Kontakten mit den bayerischen Polizeibehörden konnten mir bislang keine wesentliche Fälle genannt werden, in denen aufgrund bestehender Datenschutzvorschriften die Arbeit der Polizei beeinträchtigt worden ist, wenn von Fehlinterpretationen der Datenschutzgesetze im Einzelfall abgesehen wird. Dabei räume ich durchaus ein, daß für den Fall, daß die Datenschutzgesetze tatsächlich eine effektive Arbeit der Sicherheitsbehörden behindern würden, dies gegebenenfalls Anlaß sein müßte, einzelne Bestimmungen zu überdenken. Tatsächlich hat dieser Berufsverband auf meine Bitte, mir Beispielsfälle zu nennen, in denen selbst bei richtiger Anwendung der Datenschutzgesetze die Aufklärung von Straftaten behindert oder sogar verhindert worden ist, keine Fälle genannt. Wenn dem jedoch so ist, halte ich es für unredlich, in der Öffentlichkeit unter Berufung auf praktizierende Polizeibeamte den Eindruck zu erwecken, der Datenschutz gefährde die öffentliche Sicherheit.

5.2. Schwerpunkte meiner Tätigkeit

Folgende Schwerpunkte kennzeichnen meine Tätigkeit im Polizeibereich in den vergangenen 12 Monaten:

Prüfungen bei zahlreichen Polizeibehörden, bei denen ich auch ein Augenmerk auf das derzeit eingeführte Informationssystem der Bayerischen Polizei gerichtet habe.

Landeskriminalamt Abtlg. V
Polizeipräsidium Oberbayern
Polizeipräsidium Niederbayern/Oberpfalz
- Polizeidirektion Regensburg
- Polizeidirektion Amberg
- Polizeidirektion Weiden
- (mit nachgeordneten Dienststellen)

Polizeipräsidium Mittelfranken
- Polizeidirektion Nürnberg
- Polizeidirektion Erlangen
- Polizeidirektion Schwabach
- (mit jeweils nachgeordneten Dienstellen)

Polizeidirektion Augsburg
Polizeidirektion Krumbach

Des weiteren habe ich versucht, einen Überblick über die Informationsflüsse im Polizeibereich zu gewinnen und mich zu neu einzuführenden Automatisierungsvorhaben zu äußern. Hierzu gehörte insbesondere die Prüfung der Abteilung V im Landeskriminalamt.

Schließlich war einer der Schwerpunkte die anstehende Novellierung des Polizeirechts.

Die Ergebnisse meiner Tätigkeiten gebe ich im folgenden wieder. Dabei versuche ich in Abkehr von der bisherigen Berichterstattung durch das Aufzählen von Beispielen mein Anliegen zu verdeutlichen und nachzuweisen, daß der Datenschutzbeauftragte nicht nur theoretischen Risiken und eingebildeten Fehlhandlungen nachsinnt.

5.3. Führung und Auswertung von Kriminalakten (Bürger von 3 bis 101 Jahre)

Kriminalakten können das verfassungsrechtlich geschützte Persönlichkeitsrecht der in ihnen genannten Personen

berühren. Bei Führung dieser Akten muß daher in besonderem Maße darauf geachtet werden, daß nur richtige, im Einzelfall tatsächlich erforderliche Daten in der jeweils zulässigen Zeitspanne gespeichert und nur den berechtigten Polizeidienststellen zur Verfügung gestellt werden. Der Bayer. Verfassungsgerichtshof hat in seiner Entscheidung vom 9.7.1985 (Az.: Vf.44-VI-84) zur Führung von kriminalpolizeilichen Sammlungen ausgeführt, daß diese Aktensammlungen eine sonst für Behördenakten im allgemeinen nicht bestehende besondere, das Persönlichkeitsrecht der Bürger berührende Bedeutung hätten. Diese ergebe sich aus dem Zweck dieser Sammlungen, aus ihrem personenbezogenen Inhalt, aus dem großen Kreis der Stellen, die vom Akteninhalt Kenntnis erhalten können, aus den hierzu in Form von Dateien geführten Kriminalaktennachweisen, aus dem begrenzten Auskunftsrecht der Betroffenen und aus der Dauer der Aktenaufbewahrung. Zudem könnten gesammelte Kriminalakten ein umfangreiches, sich über einen langen Zeitraum erstreckendes Persönlichkeitsbild vermitteln. Insbesondere die Weitergabe von Auskünften aus der Aktensammlung an andere Stellen könne das Persönlichkeitsrecht des Betroffenen berühren. Die Personen, über die Kriminalakten nach Maßgabe der entsprechenden Richtlinien geführt würden, seien in ihrem allgemeinen, grundrechtlich gesicherten Persönlichkeitsrecht als schutzbedürftig anzuerkennen. Daher erscheine eine entsprechende gesetzliche Regelung geboten (siehe auch 4.2.7).

5.3.1. Kriminalaktennachweis (KAN)

Der Kriminalaktennachweis (KAN) dient dem Nachweis von Kriminalakten, die beim Bund und bei den Ländern geführt werden. Der Kriminalaktennachweis gliedert sich in einen Bundes-KAN, einen Landes-KAN und in den sogenannten regionalen KAN. Der Bundes-KAN soll sich darauf beschränken, Hinweise auf Täter besonders schwerer Straftaten oder von Straftaten mit überregionaler Bedeutung zu geben. Im Landes-KAN und im regionalen KAN werden die Kriminalakten bayerischer Polizeivollzugsdienststellen nachgewiesen. Dabei wird auch eine Kurzauskunft zu den erfaßten Sachverhalten gegeben. Eine bayerische Besonderheit ist hierbei die Aufteilung des für bayerische Kriminalakten geführten Kriminalaktennachweis in einen Landes-KAN und in einen regionalen KAN. In den bei den einzelnen Polizeidirektionen geführten regionalen KAN werden weitgehend dezentralisiert die Nachweise über Akten der Personen geführt, die lediglich auf örtlicher Polizeiebene von Bedeutung sind. Mit dieser weiteren Aufteilung des Kriminalaktennachweises soll dem Grundsatz des Datenschutzes Rechnung getragen werden, daß jede Behörde nur die Daten speichern und nur auf die Daten zugreifen darf, die sie zu ihrer gesetzlichen Aufgabenerfüllung braucht.

Wie in meinem letzten Tätigkeitsbericht angekündigt, habe ich den Aufbau der Datei „Kriminalaktennachweis" bei einigen Polizeidirektionen geprüft und dabei insbesondere darauf geachtet, ob die Abschichtung zwischen Bundes-, Landes- und regionalem KAN im vorgesehenen Sinne vollzogen wird. Als Ergebnis meiner diesbezüglichen Prüfungen bei vier Polizeidirektionen sind jedoch nicht unerhebliche Zweifel an der datenschutzgerechten Einführung des Kriminalaktennachweises im Rahmen des Informationssystems Bayerischer Polizei (IBP) festzustellen:

Zu viele Datenspeicherungen:

Zweck und Umfang kriminalpolizeilicher personenbezogener Sammlungen, zu deren Erschließung der Kriminalaktennachweis dient, ergeben sich abschließend aus den entsprechenden Richtlinien. Die Erfassung im Kriminalaktennachweis muß deshalb zur Gefahrenabwehr oder zur Strafverfolgung erforderlich sein. In Anbetracht dessen erscheint mir die Anzahl der bei den einzelnen Direktionen vorgefundenen Speicherungen als zu hoch. Bei meinen Stichproben konnte ich jeweils eine Anzahl von Fällen feststellen, in denen eine Speicherung nicht erforderlich gewesen wäre. In erhöhtem Maße haben offensichtlich die nachstehenden Delikt- und Personengruppen Schwierigkeiten bereitet.

Kinder:

Kinder sind strafunmündig. Ihre Erfassung im Kriminalaktennachweis kann nur in besonderen Ausnahmefällen gerechtfertigt sein. Der Bestand der bisher erfaßten Kinder ist zu hoch. So sind beispielsweise bei einer Polizeidirektion bis jetzt schon 620 Kinder im Kriminalaktennachweis, damit also personenbezogen erschließbar, erfaßt, obwohl erst knapp die Hälfte des Aktenbestandes über den Kriminalaktennachweis erschlossen ist. Folgende Fälle mögen als Beispiel für eine datenschutzrechtlich bedenkliche Speicherung stehen:

- Das jüngste Kind war zur Tatzeit noch nicht 4 Jahre alt. Allein wegen Ladendiebstahls war es im Landes-KAN erfaßt und somit landesweit abrufbar.
- Ein 4-jähriger Bub hat mit einem Stein an einigen Autos Kratzer angebracht.
- Ein 4-jähriger hat 1982 einen Diebstahl begangen.
- Einem weiteren 4-jährigen wird Sachbeschädigung vorgeworfen; auch hier durch Vergabe eines falschen Steuerungsmerker Einspeicherung im Landes-KAN.
- Ein 5-jähriger war bei älteren Kindern, die Straftaten begangen haben, lediglich mitgelaufen.
- Ein 5-jähriger hat ebenfalls 1982 einen Ladendiebstahl begangen.
- Einem 5-jährigem wird vorsätzliche Körperverletzung und „Mißhandlung von Schutzbefohlenen" unter 14 Jahren vorgeworfen. Beide Straftaten haben den Steuerungsmerker für den Landes-KAN. Welche Schutzbefohlenen ein 5-jähriger Bub im übrigen haben kann, erscheint zumindest fraglich.
- Ein 5-jähriger ist beim Diebstahl durch einen Älteren zufällig dabeigewesen. Der Sachverhalt wird erst 2 Jahre nach der Tat bekannt und erfaßt.
- Einem 6-jährigen wird unerlaubtes Entfernen vom Unfallort vorgeworfen.
- Fahrlässige Brandstiftung durch einen gerade 6 Jahre alt gewordenen Knaben.

Die Liste derartiger Fälle ließe sich leider fortsetzen.

Zu bemerken ist noch, daß Kinder, die im Landes-KAN gespeichert sind, gegenüber der früheren Praxis der Speicherung lediglich in Akten benachteiligt werden. War früher ein Kind wegen einer Straftat in Erscheinung getreten,

so hat dies in aller Regel keine andere Polizeidienststelle erfahren. Heute genügt eine kurze Dateianfrage, um die im Landes-KAN eingespeicherten Erkenntnisse über die Kinder landesweit zu erhalten. Dies stellt einen unbefriedigenden Zustand dar. Daher sollte auch aus diesem Gesichtspunkt mit der Einspeicherung von Kindern in den KAN mit äußerster Zurückhaltung verfahren werden.

Im übrigen sind mir bei Prüfung der im KAN gespeicherten Kinder eine Menge Erfassungsfehler aufgefallen. So waren bei einer Direktion 3 Personen gespeichert, die am Tage ihrer Geburt bereits eine Straftat begangen haben sollen. Eine andere Person war gespeichert, die ausweislich der im Kriminalaktennachweis enthaltenen Daten 22 Monate vor ihrer Geburt eine Straftat begangen haben soll.

Eine der überprüften Polizeidirektionen hat inzwischen den Bestand an Kindern auf ein knappes Sechstel der ursprünglichen Menge (19 statt 118) verringert.

Alte Bürger:

Ältere Bürger treten in der Regel nur als Täter von sogenannten Antrags- und Fahrlässigkeitsdelikten auf. Ob wegen solcher Straftaten, insbesondere wenn es sich bei den alten Menschen um „Ersttäter" handelt, eine Aufnahme in den Kriminalaktennachweis und in die entsprechenden kriminalpolizeilichen Akten wirklich erforderlich ist, sollte stets unter strengen Voraussetzungen geprüft werden. So erscheint mir auch der Bestand von 404 Personen, die älter als 75 Jahre sind, bei einer großen Direktion jedenfalls als zu hoch. Teilweise war auch die Vergabe von Aussonderungsfristen in einer Reihe von Fällen nicht nachvollziehbar und offensichtlich zu lange. In Anbetracht des hohen Alters und der Geringfügigkeit der im Einzelfall zur Last gelegten Straftat war bei vielen Leuten eine Einspeicherung in den Kriminalaktennachweis nicht gerechtfertigt. So ist eine hohe Anzahl von Erfassungen aus diesem Personenkreis ausschließlich wegen Ladendiebstahls vorhanden. Einige Beispiele mögen die zu weitgehenden Speicherungen aufzeigen:

- Eine Ordnungswidrigkeit nach dem Sprengstoffgesetz begangen durch eine 80-jährige Frau.

  Erfassung eines 75-jährigen wegen einer Ordnungswidrigkeit nach dem Tierschutzgesetz.

- Ein 76-jähriger wird wegen einer fahrlässigen Körperverletzung beim Verkehrsunfall erfaßt.

- Ladendiebstahl durch eine 81-jährige Frau. Das Verfahren wurde nach § 170 Abs. 2 Strafprozeßordnung eingestellt (kein hinreichender Tatverdacht). Im übrigen betrug der Wert der Lebensmittel 20,- DM. Die alte Frau bezieht ca. 500,- DM Rente im Monat.

- Ein 82-jähriger Mann hat in einem Supermarkt Lebensmittel von geringem Wert gestohlen. Das Verfahren war nach § 170 Abs. 2 StPO eingestellt worden.

- Zu einem 84-jährigen war der Tatbestand der „Vorbereitung eines Angriffskrieges" gespeichert.

Auch hier ließe sich leider die Liste der unzulässigen oder zumindest sehr bedenklichen Speicherungen von alten Menschen fortsetzen.

Antrags-, Fahrlässigkeits- und Privatklagedelikte:

Ganz generell stellen die Antragsdelikte (z.B. Ladensdiebstähle, Beleidigungen, einfache Körperverletzungen) einen überraschend großen Teil der erfaßten Straftaten. Obwohl die Erfassung von Antrags- und Fahrlässigkeitsdelikten, insbesondere bei Ersttätern, einem strengen Prüfungsmaßstab zu unterliegen hat, wird hier selbst bei der retrograden (rückwärtigen) Erfassung von Daten in viel zu hohem Umfang gespeichert. So umfaßt bei einer Polizeidirektion der Bestand an Antragsdelikten 1/3 aller im Kriminalaktennachweis erfaßten Straftatbestände. Der Zweck polizeilicher Datenspeicherung, nämlich Gefahrenabwehr und Verfolgung von Straftaten, wird hier wohl verkannt.

Verkehrsdelikte, Ordnungswidrigkeiten und Unfälle:

Während Verkehrsdelikte und Ordnungswidrigkeiten nur nach strenger Prüfung in Kriminalakten und somit im Kriminalaktennachweis erfaßt werden dürfen, fehlt für die personenbezogene Erfassung von Unfällen in kriminalpolizeilichen Sammlungen die entsprechende Grundlage. So ist mir bei einer Polizeidirektion aufgefallen, daß offensichtlich jede Ordnungswidrigkeit ohne nähere Prüfung personenbezogen erfaßt wird. Auch hinsichtlich der Erfassung von Verkehrsdelikten habe ich angesichts der bei Gelegenheit der Prüfung eingesehenen Akten Zweifel, ob die erforderliche Prüfung von der Polizei im ausreichenden Maße erfolgt ist. Als Beispielsfälle einer zumindest bedenklichen Erfassung sollen hier

- die Speicherung wegen Nacktbadens im Lech,
- die Speicherung von Unfallflucht begangen durch Kinder und alte Menschen,
- die Speicherung eines 74-jährigen wegen tödlichen häuslichen Unfalls,
- bei einem 12-jährigen ein „Brandfall ohne Personenschaden" genannt werden. Ich habe verlangt, daß solche Vorgänge gelöscht und künftig vergleichbare Ereignisse nicht mehr erfaßt werden.

In diesem Zusammenhang habe ich auch bei der Speicherung von Selbstmordgefährdeten und von Personen, die zu ihrem Schutz in Gewahrsam genommen werden, eine teilweise unzulässige Speicherung festgestellt. Zwar mag die Speicherung solcher Personen im Einzelfall aus polizeilicher Sicht gerechtfertigt sein, doch werden diese Vorgänge entgegen der entsprechenden polizeilichen Errichtungsanordnung so gespeichert, daß sie im Landes-KAN für 10 Jahre landesweit auskunftsfähig gespeichert werden. Ich halte grundsätzlich eine Aussonderung solcher Sachverhalte spätestens nach 2 bis 3 Jahren für erforderlich.

Die Speicherungsebenen im KAN:

Wie ich eingangs zum Kriminalaktennachweis ausgeführt habe, beruht das Konzept des Kriminalaktennachweises auf einer Abschichtung in verschiedenen Speicherungsebenen. Die Speicherung in diesen Ebenen ist entscheidend für die Frage, in welchem Bereich die einzelnen Daten abrufbar sein sollen (z.B. bundesweit, landesweit oder nur im Bereich einer Polizeidirektion). Durch Eingabe sogenannter „KAN-Merker" können Straftaten – statt nur im Landes-KAN gespeichert zu sein – zum Bundes-KAN übermittelt werden. Meine Überprüfung hat nun ergeben, daß diese KAN-Merker

unkritisch und vielfach, sowohl vom Sachverhalt als auch von der Deliktsart (Ordnungswidrigkeiten, Fahrlässigkeitsdelikte) her, unzutreffend vergeben worden sind. Damit wird aber das auch aus Datenschutzgründen notwendige KAN-Konzept unterlaufen. Als Beispiele mögen folgende Fälle einer unzulässigen Übermittlung zum Bundes-KAN dienen:

Eine Person, die vom Verdacht der einmalig begangen Freiheitsberaubung freigesprochen worden war, erhielt den KAN-Merker für „gewohnheitsmäßig" und gelangte somit in den Bundes-KAN.

- Auch ein Vermißtenfall erhielt den KAN-Merker „gewohnheitsmäßig".
- Eine Beleidigung (Antragsdelikt), die durch zwei mit zeitlichem Abstand versandte Schreiben begangen worden war, aber den gleichen Sachverhalt betroffen hatte, wurde ebenfalls als „gewohnheitsmäßig" eingestuft.
- Ein Vernehmungsersuchen für eine andere Dienststelle wurde als eigener Vorgang in den Kriminalaktennachweis eingegeben und über dies noch mit dem Merker für „planmäßig und überörtlich" versehen.
- Mehrere Personen waren mit dem KAN-Merker für „planmäßig und überörtlich" erfaßt, weil sie im Zug von München nach Augsburg ohne Fahrkarte angetroffen worden waren.
- Ein zu 80% geistig Behinderter ging von Zeit zu Zeit in Gaststätten und aß dort für ca. 10,- DM Leberkäse ohne zu bezahlen. Stets erfolgte eine Einstellung des Verfahrens nach § 170 Abs. 2 Strafprozeßordnung. Gleichwohl wurde mit der Vergabe des KAN-Merkers „gewohnheitsmäßig" die Voraussetzung für eine bundesweite Abfragemöglichkeit geschaffen.
- Das Verfahren bezüglich eines versuchten Diebstahls mit 50,- DM Schaden wurde nach § 170 Abs. 2 Strafprozeßordnung eingestellt. Dies war der einzige Vorgang zur betroffenen Person. Auch hier war die Tat als „gewohnheitsmäßig" klassifiziert worden.

Die Liste der falschen Sachbehandlungen hinsichtlich der Speicherungsebene und damit der Auskunftsfähigkeit der Daten könnte fortgesetzt werden.

Selbst die oben angesprochenen Antragsdelikte und Ordnungswidrigkeiten wurden teilweise durch Vergabe entsprechender Steuerungsmerker in den Landes-KAN oder sogar in den Bundes-KAN gesteuert. Nach der Errichtungsanordnung dürfen jedoch Ordnungswidrigkeiten ausschließlich im regionalen KAN gespeichert werden. Für Antragsdelikte gilt, daß nur unter ganz bestimmten Voraussetzungen eine Speicherung im Landes-KAN zulässig ist.

Weitere Problemfelder, die ich festgestellt habe, sind

- die teilweise zu schematische Vergabe von Aussonderungsfristen, die meist ohne Berücksichtigung der Besonderheiten des Einzelfalles erfolgt,
- die selbst bei stichprobenartiger Überprüfung aufgefallenen Erfassungsfehler – so hat z.B. eine über 80 Jahre alte Frau völlig zu Unrecht den personengebundenen Hinweis „Prostituierte" erhalten,
- die nicht vollständig durchgeführte Berichtigung von Daten, die bereits in der Testphase gespeichert worden waren, etwa die Verwendung von in der Errichtungsanordnung nicht vorgesehenen personengebundenen Hinweisen (wie vorbestraft, geschlechtskrank, Homo) und
- vermeidbare Fehler bei der retrograden Erfassung von Vorgängen.

In Anbetracht dieser aus datenschutzrechtlicher wie aus polizeilicher Sicht bedrückenden Bilanz der Prüfungen des Kriminalaktennachweises, habe ich das Bayer. Staatsministerium des Innern gebeten, dringend entsprechende Maßnahmen zur Bereinigung der bestehenden und zur Vermeidung künftiger ähnlicher Fehler zu veranlassen.

5.3.2. Überprüfung der Kriminalaktensammlungen

Eine stichprobenartige Überprüfung der Kriminalaktensammlungen bei Dienststellen im Bereich zweier Polizeipräsidien erbrachte teilweise recht unterschiedliche Ergebnisse:

So konnte ich dem Polizeipräsidium Niederbayern/Oberpfalz in Regensburg bestätigen, daß die überschlägige Überprüfung der Kriminalaktensammlungen und der dazugehörigen Suchkarteien ergeben habe, daß die Aktenaussonderung bei allen aufgesuchten Dienststellen im erfreulichen Maße auf dem laufenden ist. Nur ganz vereinzelt wurden hier Karteikarten gefunden, die nach dem auf ihnen vermerkten Aussonderungsdatum bereits hätten ausgesondert sein müssen. Ebenfalls nur vereinzelt waren auf Karteikarten keine Aussonderungsfristen eingetragen. Diese wenigen Einzelfälle, die jeweils an Ort und Stelle bereinigt wurden, haben jedoch den insgesamt positiven Eindruck vom Stand der Aktenaussonderungen nicht geschmälert.

Demgegenüber habe ich einem anderen Polizeipräsidium mitgeteilt, daß ich bei der Prüfung der noch herkömmlich erschließbaren Aktenbestände festgestellt habe, daß auf den überprüften Suchkarten weder Anlage- noch Wiedervorlagedaten eingetragen sind und damit eine sachgerechte Aussonderung wohl kaum gewährleistet sei. Einige Stichproben haben mir dies bestätigt. Als Beispiel habe ich hier folgende Fälle genannt:

- So bestand noch eine Akte über Kinder, die 1981 wegen Ladendiebstahls angelegt worden war, wobei dies das einzige Delikt war. Die Akte hätte spätestens 1983 ausgesondert werden müssen.
- Außerdem bestanden noch Karteikarten für Personen, ohne daß ein Vorgang dazu vorhanden gewesen wäre (z.B. für eine zum Prüfungszeitpunkt 101-jährige Frau).
- Seit 18 Jahren befindet sich zu einer Person als einziges ein Vorgang über ein Verfahren im Akt, das nach § 153 Abs. 2 Strafprozeßordnung (also wegen geringer Schuld) eingestellt worden war.

Ein weiterer Prüfungspunkt im Zusammenhang mit der Aktenaussonderung war jeweils auch die Frage, welche Aussonderungsfristen festgesetzt werden. Generell habe ich festgestellt (eine Ausnahme bildet die Polizeidirektion Amberg), daß die Festsetzung der Aussonderungsfristen zu schematisch gehandhabt wird. Das gleichgelagerte Problem

hatte ich auch bei der Führung der Datei zum Kriminalaktennachweis festgestellt (siehe dort). In der Regel wird ohne Prüfung des Einzelfalles für Erwachsene eine 10-Jahres-Frist, für Jugendliche eine 5-Jahres-Frist und für Kinder ein 2-Jahres-Frist festgesetzt. Eine Prüfung, ob ein Fall von geringerer Bedeutung vorliegt, der nach den entsprechenden Richtlinien grundsätzlich nach kürzerer Frist auszusondern wäre, findet offenbar kaum statt. Auch habe ich festgestellt, daß im Regelfall die Tatsache, daß ein Verfahren mit Freispruch geendet hat oder nach § 170 Abs. 2 Strafprozeßordnung eingestellt worden war, nicht zu einer Aussonderung oder zumindest wesentlichen Verkürzung der Speicherungsfristen führt. Als Beispiele einer solchen schematischen, datenschutzrechtlich jedoch unzulässigen Sachbehandlung seien kurz folgende Fälle genannt:

- Bei einer Kriminalpolizeiinspektion wurde die Akte eines 58-jährigen Mannes vorgefunden, der 1981 in einem Warenhaus eine Tafel Schokolade im Wert von 0,99 DM gestohlen hatte. Das Verfahren war von der Staatsanwaltschaft wegen Geringfügigkeit eingestellt worden. Der Mann war weder vor noch nach dem Jahre 1981 wieder in Erscheinung getreten. Die entsprechende Akte wies eine Aussonderungsfrist von 10 Jahren auf.

- Bei einer Polizeiinspektion war eine Akte über eine Person angelegt, die im Jahre 1981 in einer Bar im betrunkenen Zustand einer anderen Person mit der Hand ins Gesicht geschlagen hatte. Der Geschlagene hatte keinen Strafantrag gestellt. Die Staatsanwaltschaft hat mangels Strafantrags und mangels öffentlichen Interesses das Verfahren eingestellt. Auch diese Person war weder vor noch nach dieser Tat weiter polizeilich in Erscheinung getreten. Auch hier war eine Aussonderungsfrist von 10 Jahren festgesetzt worden.

Eine Nachprüfung beim Bayerischen Landeskriminalamt hat ergeben, daß auch im bereinigten Aktenbestand wohl nach wie vor fehlerhafte Speicherungen vorliegen. So fanden sich Vorgänge mit falschen Prüfungsfristen oder Einzelfälle, in denen der Akteninhalt eine Speicherung in der entsprechenden Aktensammlung nicht gerechtfertigt hat. Das Landeskriminalamt hat inzwischen mit einer Nachbereinigung des Aktenbestandes begonnen. Dies begrüße ich.

5.3.3. Kriminalaktensammlung beim Polizeipräsidium München

Im 6. Tätigkeitsbericht hatte ich mitgeteilt, daß nach Auskunft des Polizeipräsidiums München die dortige Kriminalaktensammlung derzeit einen Bestand von 1 Mio. personenbezogener Akten umfasse. Diese Zahl hatte ich als zu hoch kritisiert und gefordert, daß die Aktenbereinigung stark beschleunigt werden muß. Auf meine Bitte um Mitteilung, welche Maßnahmen in der Zwischenzeit vom Polizeipräsidium zur Bereinigung des Aktenbestandes geplant und ergriffen worden sind und wie hoch derzeit der aktuelle Bestand an Kriminalakten tatsächlich ist, hat das Polizeipräsidium München berichtet, daß aufgrund einer zwischenzeitlichen durchgeführten Zählung nur ein Bestand von rund 500.000 Akten festgestellt worden sei. Die Zahl von einer 1 Mio. Akten habe lediglich auf einer Schätzung beruht. Im übrigen sei das Polizeipräsidium weiterhin bestrebt, die Aussonderung der Kriminalakten entsprechend den einschlägigen Richtlinien zügig fortzusetzen.

Zwar bin ich einerseits erleichtert, daß im Polizeipräsidium München nicht, wie zunächst angegeben, 1 Mio. Kriminalakten vorgehalten werden und weiterhin zügig ausgesondert wird. Allerdings bin ich doch befremdet, wie wenig genau gelegentlich Anfragen meiner Dienststelle beantwortet werden. Nach Art. 28 Abs. 1 Satz 2 Bayer. Datenschutzgesetz sind mir zur Erfüllung meiner Aufgaben alle notwendigen Auskünfte zu geben. Meine Tätigkeit wird wesentlich erschwert, wenn Antworten wie im vorliegenden Fall über die Höhe eines Aktenbestandes um 100% von den tatsächlichen Verhältnissen abweichen. Bei meiner datenschutzrechtlichen Beurteilung von Sachverhalten bin ich nun einmal auf die gesetzlich gebotene Mithilfe der Behörden angewiesen.

5.4. Neuordnung der polizeilichen Meldewege

Zur Verbesserung der Information der einzelnen Polizeidienststellen, zum Erkennen überörtlicher Täter, zur Aufklärung von Straftaten, zum rechtzeitigen Handeln in Gefährdungssituationen und zur Konzentrierung polizeilicher Tätigkeit sind in den vergangenen Jahrzehnten eine Reihe von polizeilichen Meldewegen, insbesondere von sogenannten Meldediensten eingerichtet worden. Mit verschiedenen Meldungen sollen Polizeidienststellen auf gleicher Ebene, aber auch vorgesetzte Dienststellen oder das Landeskriminalamt als bayerische Zentralbehörde und auch das Bundeskriminalamt von Vorgängen unterrichtet bzw. nach etwa dort vorliegenden Erkenntnissen befragt werden. Ohne daß hier die einzelnen Meldedienste vollständig aufgeführt werden könnten, gibt es Mitteilungen über bekannte und unbekannte Täter, über erkennungsdienstliche Behandlungen, Meldungen in Staatsschutzangelegenheiten und anderen Kriminalitätsbereichen, Erkenntnisanfragen, Meldungen über wichtige Ereignisse und Lage- oder Tagesmeldungen.

Eine Prüfung der Informationsverarbeitung im Bayerischen Landeskriminalamt, dem nach Art. 7 Polizeiorganisationsgesetz neben einigen Aufgaben als Verfolgungsbehörde auch die Aufgabe als Zentralbehörde zugewiesen ist, hat ergeben, daß die bisherige Einführung von automatisierten polizeilichen Dateien weitgehend ohne Auswirkungen auf die bisherigen Meldedienste geblieben ist. Dies wiederum hat zur Folge, daß Meldedienste fortbestehen, obwohl ihre Funktionen weitgehend durch Dateien und entsprechende Abfragemöglichkeiten ersetzt worden sind. Dies kann in einzelnen Fällen zu überflüssigen Doppelspeicherungen oder Mehrfachübermittlung von Daten führen.

Insbesondere die Einführung der Kriminalaktennachweisdatei in Bayern wird wohl grundsätzlich dazu führen, daß sogenannte **Erkenntnisanfragen** zwischen Polizeibehörden nicht mehr erforderlich sind. Diese Erkenntnisanfragen, also die Frage an eine andere Polizeidienststelle nach Erkenntnissen beispielsweise über einen Verdächtigen, hat im Einzelfall nicht nur zu einer Übermittlung etwa vorhandener Erkenntnisse, sondern vielfach auch zu einer Anlage von personenbezogen erschlossenen Unterlagen bei den angefragten Dienststellen geführt. Insbesondere das Landeskriminalamt hat wegen seiner Zentralstellenfunktion die im Wege von Erkennnisanfragen seinerseits erlangten Erkenntnisse in personenbezogen geführten Akten in einem automatisierten Verfahren erschließbar gespeichert. Diese

Doppelspeicherung bei sachbearbeitender Polizeidienststelle und Landeskriminalamt zeigt insbesondere mit Einführung des Kriminalaktennachweises Probleme. Wird eine Erkenntnisanfrage zu einer Person an das Landeskriminalamt versandt, die einer Bagatellstraftat verdächtig ist, so wird über die Aktenanlage im Landeskriminalamt der Vorgang vom Grundsatz her landesweit verfügbar. Nach den Richtlinien zum Kriminalaktennachweis sollte das Delikt jedoch nur regional im Umkreis der sachbearbeitenden Polizeibehörde abfragbar sein. Damit wird das Konzept des Kriminalaktennachweises unterlaufen. Das Landeskriminalamt hat auf meine Feststellungen hin erste Konsequenzen gezogen, um in diesem Punkt für die Übergangszeit bis zur endgültigen landesweiten Einführung des Kriminalaktennachweises eine Umgehung der entsprechenden Richtlinien zu vermeiden.

Zu den **Erkenntnisanfragen** und der darin enthaltenen Übermittlung personenbezogener Daten über Betroffene eines Strafverfahrens habe ich zudem festgestellt, daß eine größere bayerische Polizeibehörde beispielsweise auch wegen sogenannter Bagatell-Delikte (z.B. Ladendiebstählen) Erkenntnisanfragen offenbar schematisch an das Bundeskriminalamt und das Bayerische Landeskriminalamt richtet. Einen Nutzen für die weitere polizeiliche Sachbearbeitung kann ich bei dieser Art von Anfragen nicht erkennen. Darüber hinaus ist die Bezeichnung der Straftat oft nicht ausreichend genug, um den angefragten Dienststellen die Möglichkeit einer sachgerechten Entscheidung über eine eventuelle Aktenanlage zu geben. Ich habe in einigen Fällen den Eindruck gewonnen, daß die Erkenntnisanfragen nicht zur Erholung von Erkenntnissen gedient haben, sondern – allerdings unter falscher Bezeichnung – zur Übermittlung von personenbezogenen Daten, für die sich eine andere den Vorgang rechtfertigende Grundlage nicht finden läßt.

Ich habe auch hier das Innenministerium gebeten, bei den nachgeordneten Dienststellen darauf hinzuwirken, daß Erkenntnismitteilungen nur auf bedeutsame Ermittlungsverfahren beschränkt werden und die vorstehend geschilderte Übung abgestellt wird.

Das vergleichbare Problem, das durch die vorschriebene Übermittlung **erkennungsdienstlicher Unterlagen** über das Landeskriminalamt an das Bundeskriminalamt entsteht, scheint derzeit nicht lösbar zu sein. Eine Neuordnung der entsprechenden Übermittlungen und Speicherungen wird wohl erst dann vorgenommen werden, wenn die entsprechende Inpol-Datei für erkennungsdienstliches Material beim Bundeskriminalamt eingerichtet sein wird. Auf die allerdings dann entstehenden Überschneidungen zwischen Kriminalaktennachweis und Datei über erkennungsdienstliche Daten habe ich schon früher hingewiesen (siehe auch unten „Erkennungsdienstliche Behandlung").

Zu den sogenannten **„Lage- oder Tagesmeldungen"** ist folgendes zu bemerken: Meines Wissens werden die Verbreitung und der Inhalt dieser Meldungen durch die jeweiligen Polizeipräsidien selbst geregelt und sollen der Erhebung der Sicherheitslage und dem Nachrichtenaustausch für polizeiliche Zwecke dienen. Die Meldungen werden durch bestimmte festgelegte Verteiler im eigenen und in den angrenzenden Präsidialbereich, in den Direktionsbereichen, an das Landeskriminalamt und auch in andere Bundesländer gesteuert. Der Inhalt dieser Meldungen läßt allerdings meines Erachtens teilweise einen sinnvollen Bezug zur effektiven polizeilichen Tätigkeit vermissen und dürfte zur Erfüllung der Ziele „Erhebung der Sicherheitslage und Fahndung und Ermittlung überörtlicher Täter" nicht geeignet sein. So hat zum Beispiel eine Polizeidienststelle dem Landeskriminalamt, vier Polizeidirektionen und dem zuständigen Polizeipräsidium mitgeteilt, daß der Bürger H. wegen Volltrunkenheit in Schutzgewahrsam genommen und der Rentner A. zwei Schachteln Zigaretten im Wert von DM 7,- im Supermarkt entwendet hat.

Somit werden auf diese Weise auch personenbezogene Daten einem großen Empfängerkreis zugänglich, ohne daß dies wirklich erforderlich wäre. Auch liegt in diesen Meldungen eine der Ursachen, daß in Teilbereichen das Prinzip der Abschottung des Kriminalaktennachweises umgangen wird.

Vorgangsverwaltung statt kriminalpolizeiliche Akten

Als ein Ergebnis meiner Überprüfungen der Informationsverarbeitung beim Landeskriminalamt habe ich festgestellt, daß die dortigen über ein automatisiertes Verfahren erschließbaren personenbezogenen Akten vielfach Vorgänge enthalten, die nur Belege etwa für die Beantwortung von Erkenntnisanfragen oder für die Weiterleitung von Informationen an andere Polizeibehörden enthalten. Sie sind somit in erster Linie Nachweise für die Verwaltungstätigkeit des Landeskriminalamtes. Einen darüber hinaus gehenden eigenständigen kriminalpolizeilichen Informationsgehalt haben diese Unterlagen vielfach nicht. Somit sind diese Akten und die diese erschließende automatisierte Datei zum Teil nur Registraturnachweis von Vorgängen. Für diese Zwecke erscheint mir allerdings eine Vorgangsverwaltung das geeignetere Instrument zu sein. Eine personenbezogene über eine automatisierte Datei erschließbare Speicherung in kriminalpolizeilichen Akten ist aus Datenschutzgründen insoweit unzulässig. Ich habe im übrigen das Landeskriminalamt darauf hingewiesen, daß der Rahmen für die Verarbeitung der Daten in einer Vorgangsverwaltung nach folgenden Kriterien zu bestimmen ist: Durch den zulässigen Informationsgehalt des Kriminalaktennachweises, wie er sich derzeit aus den entsprechenden Richtlinien und Anordnungen ergibt, und durch die gesetzliche Zuständigkeit des Landeskriminalamtes, insbesondere in dessen Funktion als Zentralstelle. Dabei wird insbesondere zu prüfen sein, wieweit neben einer entsprechenden Vorgangsverwaltung und neben dem Kriminalaktennachweis noch Raum für eine weitere Aktenhaltung und eine diese erschließende automatisierte Datei beim Landeskriminalamt bleibt. Jedenfalls müßten die Dateien des Landeskriminalamtes bei weitgehender Vermeidung von Doppelspeicherungen unter Berücksichtigung ihrer jeweils unterschiedlichen Aufgabenstellung aufeinander abgestimmt sein.

Das Bayerische Landeskriminalamt hat auf meine diesbezüglichen Vorschläge außerordentlich schnell reagiert und mitgeteilt, daß entsprechend meinen Vorschlägen eine Vorgangsverwaltung eingerichtet wird. Dies begrüße ich. Ich hoffe, daß hiermit ein Weg gefunden ist, der bei Wahrung der schutzwürdigen Interessen der Betroffenen vor unnötiger Speicherung in personenbezogenen Dateien und Akten dem Landeskriminalamt eine sachgerechte und praxisnahe Erledigung seiner Aufgaben ermöglicht.

5.5. Personengebundene Hinweise

In polizeilichen Informationssystemen, wie zum Beispiel im INPOL-Verbund-System und in der Datei „Kriminalaktennachweis", werden personengebundene Hinweise verwendet. Im 6. Tätigkeitsbericht hatte ich auf dieses Problem im Zusammenhang mit der Verwendung des Begriffes „Zigeunername" hingewiesen. Diese Hinweise sollen u.a. folgenden Zwecken dienen:

- Eigensicherung des einschreitenden Beamten,
- Einleitung gezielter Fahndungsmaßnahmen,
- Unterstützung der polizeilichen Ermittlungen und
- zum Schutz des Betroffenen bei polizeilichen Maßnahmen.

Personengebundene Hinweise sind also Daten, die über die Identifizierungsfunktion hinausgehen und eine erste Einschätzung der gespeicherten Person ermöglichen sollen.

Ich habe keinen Zweifel, daß einzelne personengebundenen Hinweise insbesondere in Fahndungsdateien allein schon für die berechtigte Eigensicherung des einschreitenden Beamten erforderlich sind. Beispielsweise muß der Polizeibeamte, der einen ausgeschriebenen Straftäter festnehmen will, darüber unterrichtet sein, ob der Straftäter in früheren Fällen bewaffnet aufgetreten oder als gewalttätig bekannt ist. Problematischer kann dies jedoch schon dann sein, wenn personengebundene Hinweise, wie Ansteckungsgefahr, geistesschwach, entmündigt, Prostitution, aus Dateien ausgegeben werden, die zum Aktennachweis angelegt sind. Beim Abruf dieser Dateien ist im Regelfall eine kurzfristige Kenntnis solcher Tatbestände nicht erforderlich. Das Risiko scheint mir nicht völlig ausgeschlossen zu sein, daß die Speicherung derartiger Hinweise die Gefahr der Ergreifung polizeilicher Maßnahmen ausschließlich aufgrund des Dateiinhaltes hervorruft und daß diese Hinweise ganz allgemein zu einer sozialen Abstempelung der betroffenen Person führen können. So bin ich der Ansicht, daß polizeiliche Entscheidungen und polizeiliches Einschreiten grundsätzlich nicht auf den Inhalt von solchen Hinweisen in polizeilichen Nachweisdateien gestützt werden dürfen, sondern daß im Regelfall zunächst Auskunft aus der polizeilichen Akte eingeholt werden muß. Die personengebundenen Hinweise sind keine geeignete Entscheidungsgrundlage, weil sie im Gegensatz zum Akteninhalt eben nur bruchstückhafte Informationen darstellen und – dies scheint mir ein besonders wichtiger Gesichtspunkt – ihre ständige Aktualisierung nicht gewährleistet ist. Gerade im letzteren Fall besteht dann das Risiko, daß aufgrund falscher Daten Entscheidungen getroffen werden. Um die möglichen Gefahren bei nur auf die personengebundenen Hinweise gestützten Entscheidungen zu verdeutlichen, verweise ich auf einen bei der Prüfung des Kriminalaktennachweises festgestellten Erfassungsfehler:

> Aufgrund fehlerhafter Eingabe war eine 80-jährige Frau mit dem personengebundenen Hinweis „Prostitution" zu Unrecht verknüpft worden. Im konkreten Fall mag man diesen Fehler als nicht sehr bedeutend ansehen, da er wohl bei einer 80-jährigen Frau offenkundig ist. Dieser Fehler hätte aber aufgrund der Art seiner Entstehung auch bei einer jungen Frau geschehen können. Der Schaden für das Ansehen, der in einem solchen Fall jedoch eintreten könnte, kann ungemein groß sein.

Deshalb meine ich, daß die Verwendung personengebundener Hinweise in automatisierten Dateien wegen der nun einmal damit verbundenen Risiken nur dann zulässig sein sollte, wenn diese zur Erreichung des mit der einzelnen Datei verfolgten polizeilichen Zwecks im jeweiligen Einzelfall unabdingbar ist. Weiter muß aber sichergestellt sein, daß sich die Richtigkeit dieser Hinweise aus Unterlagen belegen läßt und diese Daten regelmäßig auf ihre Aktualität überprüft werden. Auch bei der Einstellung personengebundener Hinweise in polizeiliche Dateien ist im Einzelfall zwischen den berechtigten Datenschutzbelangen der möglicherweise betroffenen Bürger – dies sind keineswegs nur Straftäter – und den Belangen der öffentlichen Sicherheit und Ordnung abzuwägen.

5.6. Erkennungsdienstliche Behandlung

Die Polizei kann Bürger erkennungsdienstlich behandeln, wenn dies etwa für Zwecke der Gefahrenabwehr (Art. 13 Polizeiaufgabengesetz) oder für Zwecke der Strafverfolgung notwendig ist (§ 81 b Strafprozeßordnung). Bereits in meinem 4. Tätigkeitsbericht habe ich darauf hingewiesen, daß die Speicherung erkennungsdienstlicher Unterlagen nur zulässig ist, wenn die ursprüngliche erkennungsdienstliche Behandlung nach den entsprechenden gesetzlichen Bestimmungen rechtmäßig war und die weitere Aufbewahrung des Materials für die jeweilige Aufgabenerfüllung erforderlich ist. Grundsätzlich gilt, daß sich die Grenzen für die Berechtigung der Polizeibehörde zur Aufbewahrung erkennungsdienstlicher Unterlagen im Einzelfall aus deren Zweckbestimmung ergeben. Auf der anderen Seite muß beachtet werden, daß der Betroffene durch die Aufbewahrung dieser Unterlagen in seiner persönlichen Sphäre schon allein wegen des Bewußtseins betroffen ist, von der Kriminalpolizei als potentieller Rechtsbrecher betrachtet zu werden. Die Aufbewahrung kann infolge dessen nur so lange gerechtfertigt sein, wie nach der konkreten Sachlage Anhaltspunkte dafür vorliegen, daß die erkennungsdienstlich behandelte Person auch zukünftig strafrechtlich in Erscheinung treten könnte und die angefertigten Unterlagen für die Ermittlung der Polizei förderlich sind (vgl. BVerwGE, Bd. 26, S. 171).

Stichproben bei Polizeidienststellen im Berichtszeitraum haben nun ergeben, daß insbesondere im Bereich des Polizeipräsidiums München und der Polizeidirektion Nürnberg erkennungsdienstliche Behandlungen in großer Zahl durchgeführt worden sind, denen lediglich Delikte der sogenannten „Bagatell-Kriminalität" zugrunde gelegen waren. Ich bin mir nicht hinreichend sicher, ob hier tatsächlich stets die gesetzlichen Voraussetzungen von § 81 b Strafprozeßordnung oder von Art. 13 Polizeiaufgabengesetz vorgelegen haben. Eher erscheint mir hier ein gewisser Schematismus vorzuliegen.

> Denn es ist jedenfalls bei einer Vielzahl von Fällen nicht ersichtlich, warum jeweils wegen Beleidigung, Beförderungserschleichung, Sachbeschädigung eine erkennungdienstliche Behandlung durchgeführt worden war.

Bei der Bedeutung dieser Angelegenheit ist auch zu berücksichtigen, daß Unterlagen solcher erkennungsdienstlicher Behandlungen über das Landeskriminalamt auch an das Bundeskriminalamt gelangen und nicht selten den nationalen Interpol-Zentralbüros anderer Staaten mitgeteilt werden. Auch steht die Tatsache der polizeilichen Erfassung wegen einer erkennungsdienstlichen Behandlung den Polizeidienststellen anderer Bundesländer über deren für den Bestand des Bundeskriminalamtes abfrageberechtigten Terminals auskunftsfähig zur Verfügung. Dieses ist um so mehr bedenklich, wenn, wie häufiger festgestellt, eine solche erkennungsdienstliche Behandlung den einzigen Grund der Erfassung darstellt und darüber hinaus Delikte betrifft, die nach den Regeln der Kriminalaktennachweis-Errichtungsanordnung (siehe dort) nur regional oder allenfalls landesweit zur Verfügung stehen dürften.

Ich habe das Landeskriminalamt deswegen gebeten, das eingehende erkennungdienstliche Material dahingehend zu überprüfen, ob nach dem mitgeteilten Sachverhalt eine erkennungsdienstliche Behandlung offensichtlich zulässig oder unzulässig war. Nur im ersteren Falle dürften meines Erachtens die erkennungsdienstlichen Unterlagen beim Landeskriminalamt gespeichert und an das Bundeskriminalamt übermittelt werden. Diese Verpflichtung zur Prüfung hat das Landeskriminalamt grundsätzlich anerkannt. Allerdings beachten manche bayerischen Polizeidienststellen bei der Übermittlung von erkennungsdienstlichem Material an das Landeskriminalamt nicht die entsprechenden Richtlinien, die vorschreiben, daß Anlaß und Rechtsgrundlage der erkennungsdienstlichen Behandlung anzugeben sind.

Wird bei der Polizei erkennungsdienstliches Material vernichtet, bedeutet dies, daß keinerlei Unterlagen (Fingerabdrücke, Lichtbilder) mehr für erkennungsdienstliche Zwecke vorhanden sein dürfen. Die Vernichtung schließt jedoch auch eine weitgehende Löschung von Hinweisen auf die ausgesonderte ed-Behandlung und die weitere Verwendung „vernichteter" Unterlagen ein. Damit nicht vereinbar ist jedoch eine von mir festgestellte Verfahrensweise des Bundeskriminalamtes (BKA): Ein in München ed-behandelter Bürger hatte die Vernichtung der zu seiner Person vorliegenden ed-Unterlagen gerichtlich durchgesetzt. Daraufhin waren diese Unterlagen in Bayern und auch beim BKA vernichtet worden. Gleichwohl hat das BKA zu einem späteren Zeitpunkt auf eine Anfrage des Bayer. Landeskriminalamtes nach eventuellen Erkenntnissen zu dieser Person folgendes mitgeteilt: „Bestand über die Vernichtung von ed-Unterlagen, aufgenommen am 14.2.1982 beim PP München wegen Verdacht des ..."

Offensichtlich wurde beim BKA die Tatsache der Vernichtung von ed-Material personenbezogen aufbewahrt. Durch diese Sachbehandlung und durch die Unterrichtung anderer Polizeidienststellen wird der mit der Vernichtung angestrebte Zweck unterlaufen.

Aufgrund dieser Erkenntnisse habe ich das Bayerische Staatsministerium des Innern gebeten, die Polizeidienststellen auf die Beachtung der entsprechenden Richtlinien zu erkennungsdienstlichen Behandlungen hinzuweisen.

5.7. Novellierung des Polizeirechts

Bereits in meinem 6. Tätigkeitsbericht habe ich die Forderung erhoben, daß für die Verarbeitung personenbezogener Daten durch die Polizei eine gesetzliche Regelung erforderlich ist. Auch die Innenministerkonferenz hat auf ihrer Sitzung am 30.6.1984 die Notwendigkeit von einheitlichen Rechtsvorschriften in Bund und Ländern für die polizeiliche Datenverarbeitung hervorgehoben und den hierfür zuständigen Arbeitskreis II beauftragt, baldmöglichst einen Entwurf nebst Begründung mit bereichsspezifischen Regelungen für die polizeiliche Datenerhebung und -verarbeitung vorzulegen. Dies hat der Arbeitskreis inzwischen getan (siehe unten „Änderung des Musterentwurfs").

Die Notwendigkeit gesetzlicher Regelungen für die polizeiliche Datenverarbeitung wird durch die Entscheidung des Bayer. Verfassungsgerichtshofes vom 9.7.1985 (Az.: Vf.44-VI-84) bestätigt. Das Gericht hat in dieser Entscheidung zu Verfassungsrechtsfragen im Zusammenhang mit der Führung und Auswertung von kriminalpolizeilichen Sammlungen festgestellt, daß es nach Art. 101 i.V.m. Art. 100 Bayer. Verfassung geboten erscheine, daß der Gesetzgeber die Materie regelt, die bisher Gegenstand der KpS-Richtlinien ist. Die derzeit bestehende Regelungslücke müsse allerdings für eine gewisse Übergangszeit hingenommen werden, um dem Gesetzgeber ausreichend Zeit für die Beratung und den Erlaß der erforderlichen Vorschriften zu lassen.

Aufeinanderabstimmen der Gesetze

Meines Erachtens ist es wesentlich, daß die Regelungen für die Datenverarbeitung im Sicherheitsbereich aufeinander abgestimmt sind. Das bedeutet, daß nicht nur Polizeigesetze, Verfassungsschutzgesetze und die Strafprozeßordnung hinsichtlich ihrer Regelungen zur Datenverarbeitung aufeinander abgestimmt sein müssen, sondern daß auch die bereichsspezifischen Regelungen in speziellen Gesetzen wie dem Sozialgesetzbuch, dem Straßenverkehrsrecht oder dem Melderecht, soweit sie die Datenverarbeitung durch Sicherheitsbehörden betreffen, in den grundsätzlichen Regelungen nicht widersprüchlich sein dürfen. Die Datenschutzbeauftragten der Länder und des Bundes haben anläßlich der Konferenz am 24. Januar 1985 einen Beschluß zu den „Anforderungen an Datenschutzregelungen im Polizeirecht" gefaßt. Neben der nochmaligen Wiederholung der Notwendigkeit bereichsspezifischer Regelungen haben die Datenschutzbeauftragten folgende Grundsätze für die polizeiliche Informationsverarbeitung festgestellt. Diese sind im folgenden im Wortlaut wiedergegeben:

Grundsätze polizeilicher Informationsverarbeitung
Allgemeine Prinzipien

Die gesetzlichen Regelungen über die Informationsverarbeitung müssen die polizeilichen Befugnisse klar und rechtsstaatlich umschreiben. Dies bedeutet

- dem Gebot der Normenklarheit entsprechende Spezialregelungen und damit die Zurückdrängung von Generalklauseln,
- Beachtung des Grundsatzes der Verhältnismäßigkeit,
- prinzipielle Beschränkung auf die Aufgaben Gefahrenabwehr und Strafverfolgung,
- Beachtung des Grundsatzes der Zweckbindung der Daten.

In Übereinstimmung mit dem vom Bundesverfassungsgericht anerkannten Recht auf informationelle Selbstbestimmung müssen die Regelungen jede Art und Form der Verarbeitung personenbezogener Daten durch die Polizei erfassen.

Sowohl die Erhebung als auch jede Nutzung von Daten sind in die Regelung mit einzubeziehen.

Die Form der Verarbeitung ist bei der Intensität der einzelnen Regelung zu berücksichtigen.

Die Speicherung personenbezogener Merkmale wie Krankheit oder besonderer Verhaltensweisen, insbesondere mit Hilfe automatischer Verfahren, ist nur zulässig, wenn die möglichen Verwendungen in einem angemessenen Verhältnis zu den Gefahren für die schutzwürdigen Belange der Betroffenen stehen. Durch die Automatisierung darf keine Verzerrung oder unangemessene Verkürzung des Sachverhalts entstehen.

Für die Datenverarbeitung sollten folgende Grundsätze Beachtung finden:

Zum **Erheben** und **Speichern** personenbezogener Daten

Grundsätze

Die Verarbeitung von Daten muß grundsätzlich der Abwehr einer im einzelnen Fall bestehenden (konkreten Gefahr) oder der Aufklärung einer konkreten Straftat dienen.

- Eine darüber hinausgehende Verarbeitung kann nur in eng begrenzten Fällen zugelassen werden. Insbesondere bedürfen Befugnisse zur vorbeugenden Bekämpfung von Straftaten einer klaren abschließenden Umschreibung im Gesetz.
- Für die Erfüllung spezialgesetzlich zugewiesener Aufgaben stehen der Polizei nur die jeweiligen spezialgesetzlichen Befugnisse zu.
- Der Bürger muß – wie zuletzt auch das Bundesverfassungsgericht im Volkszählungs-Urteil festgestellt hat – grundsätzlich unbeobachtet von staatlichen Stellen an Versammlungen teilnehmen können. Bei Befugnissen zur Informationserhebung in Versammlungen ist stärker als in der bisherigen Praxis dem Grundrecht der Versammlungsfreiheit Rechnung zu tragen.

Werden personenbezogene Informationen in Dateien gespeichert, müssen die Herkunft und die Richtigkeit der Informationen in Akten oder anderen Unterlagen nachweisbar sein. Werden Bewertungen gespeichert, muß erkennbar sein, wer die Bewertungen vorgenommen hat und wo die Erkenntnisse gespeichert sind, die ihnen zugrundeliegen.

Datenerhebung und **-speicherung**

- Die Gewinnung von Informationen muß grundsätzlich offen geschehen; heimliche Informationserhebung ist nur dann zulässig, wenn dies zur Aufgabenerfüllung im Einzelfall unerläßlich ist.
- Die Erhebung durch selbsttätige Lese- und Aufzeichnungsgeräte ist gesetzlich zu regeln.
- Bei Erhebung von Daten unter Mitwirkung des Betroffenen ist dieser in der Regel auf seine Aussage- oder Mitwirkungspflicht oder auf die Freiwilligkeit hinzuweisen.
- Werden heimlich erhobene Daten gespeichert, ist der Betroffene grundsätzlich nach Wegfall der Zweckgefährdung zu informieren.
- Die Anfertigung und Aufbewahrung erkennungsdienstlicher Unterlagen muß präziser und restriktiver geregelt werden. Vorschriften über die Anfertigung und Verarbeitung von erkennungsdienstlichen Unterlagen dürfen nicht durch neue technische Möglichkeiten umgangen werden (z.B. Überwachung bestimmter Orte durch Videogeräte, automatische Stimmerkennung).
- Die Übernahme der in Strafermittlungsverfahren erhobenen Informationen in Unterlagen für Zwecke der Gefahrenabwehr und vorbeugenden Bekämpfung von Straftaten ist an strenge Voraussetzungen zu knüpfen.
- Der Abgleich von oder mit Fremddatenbeständen darf künftig nur zur Abwehr erheblicher gegenwärtiger Gefahren sowie zur Aufklärung abschließend festgelegter schwerer Straftaten zugelassen werden. Die hierbei gewonnenen Daten müssen einer strengen Zweckbindung unterliegen. Voraussetzungen, Art und Umfang des Abgleichs, Verwertung und Dauer der Aufbewahrung sind im Gesetz abschließend zu regeln.
- Der Einsatz besonderer Verfahren, die über ein Aktenhinweissystem hinausgehen (z.B. Spurendokumentationsverfahren), bedarf einer gesetzlichen Regelung.
- Personenbezogene Daten dürfen grundsätzlich nur bei der sachbearbeitenden Dienststelle in kriminalpolizeilichen Sammlungen oder entsprechenden Dateien gespeichert werden. Die Speicherung dieser personenbezogenen Daten bei polizeilichen Zentralstellen ist nur aufgrund ausdrücklicher gesetzlicher Regelung zulässig.
- Erkenntnisanfragen oder Bitten um Amtshilfe dürfen bei den angefragten Stellen grundsätzlich nicht zur Anlage kriminalpolizeilicher Personenakten oder -dateien führen. Gleiches muß für bloße Unterrichtungen gelten.

Übermittlung von Daten

Die zu polizeilichen Zwecken gewonnenen Daten sind grundsätzlich zweckgebunden zu verwerten.

Bei der Übermittlung an Polizeibehörden ist hinsichtlich Art und Inhalt nach der konkreten polizeilichen Funktion und Zuständigkeit zu unterscheiden. Die Datenübermittlung an zentrale Stellen ist restriktiv zu regeln; das gilt auch für Erkenntnisanfragen und deren Beantwortung.

Eine Übermittlung an andere als Polizeibehörden und sonstige öffentliche Stellen sowie an Privatpersonen ist nur im Einzelfall zulässig und nur

- zur Abwendung einer konkreten Gefahr, einer erheblichen sozialen Notlage oder
- zur Verfolgung von öffentlich-rechtlichen oder zivilrechtlichen Ansprüchen in Fällen von Beweisnot,

und nur, wenn hierfür eine ausdrückliche gesetzliche Regelung besteht. Bei Anfragen, deren Beantwortung in die Zuständigkeit anderer Stellen fällt, hat die Polizei grundsätzlich an diese Stellen zu verweisen. Die Vorschriften des Bundeszentralregistergesetzes dürfen nicht durch polizeiliche Auskunft unterlaufen werden.

Eine Datenübermittlung an Nachrichtendienste darf wegen der verfassungsrechtlich gebotenen Trennung von polizeilicher und nachrichtendienstlicher Tätigkeit entgegen der derzeitigen Praxis nur in engen Grenzen zugelassen werden. Ein geeigneter Maßstab sind die Übermittlungsregelungen nach dem Gesetz zu Art. 10 GG.

Bei der Übermittlung an ausländische Stellen ist durch geeignete Absprachen und durch die Vereinbarung internationaler Regelungen sicherzustellen, daß die innerstaatlichen Grundsätze des Datenschutzes nicht gefährdet werden.

Vor jeder Übermittlung hat die auskunftgebende Stelle grundsätzlich die Richtigkeit der vorhandenen Unterlagen und deren Erforderlichkeit für die eigene Aufgabenerfüllung zu überprüfen. Wenn ein Verfahren noch nicht abgeschlossen ist, ist darauf hinzuweisen. Eine Übermittlung hat zu unterbleiben, wenn die Unterlagen zu vernichten sind.

Tatsache und Inhalt der Übermittlung sind in der Akte festzuhalten. Bei Veränderung wesentlicher Gesichtspunkte (z.B. Löschung) hat die übermittelnde Stelle die Änderung nachzuberichten, soweit dadurch nicht schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Löschungs- und Überprüfungsvorschriften

Für die Aufbewahrung der Daten muß der Gesetzgeber differenzierte Löschungs- und Überprüfungsvorschriften gesetzlich vorsehen. Insbesondere ist zu unterscheiden

- nach Alter des Betroffenen,
- nach der Schwere der Gefahr und der Straftat,
- nach der Art der Tatbegehung,
- nach der Art der Daten,
- nach dem Ausgang des Verfahrens.

Die gegenwärtig praktizierten Regelfristen (für Kinder 2 Jahre, für Jugendliche 5 Jahre, für Erwachsene 10 Jahre) dürfen nicht verlängert werden.

Daten, die allein zur Personenfeststellung erhoben wurden, sind unmittelbar nach Zweckerreichung zu vernichten.

Transparenz

Entsprechend der verfassungsmäßigen Garantie des Rechtsweges (Art. 19 Abs. 4 GG) hat der einzelne grundsätzlich ein Recht auf vollständige Auskunft. Dieses umschließt

- die zu seiner Person gespeicherten Informationen,
- Zweck, Rechtsgrundlage und vorgesehene Dauer der Speicherung,
- Art der Gewinnung oder Herkunft der Informationen,
- die Tatsache und den Inhalt der Übermittlung an andere Stellen.

Ausnahmen hiervon sollten nur dann zulässig sein, wenn hierdurch die Erfüllung polizeilicher oder anderer Sicherheitsaufgaben gefährdet oder erheblich erschwert wird, überwiegende Interessen Dritter entgegenstehen oder die Erfüllung des Auskunftsanspruchs nur mit unverhältnismäßigem Aufwand möglich wäre.

Die Bearbeitung von Auskunftsersuchen muß getrennt von polizeilichen Informationssammlungen erfolgen. Die Tatsache der Antragstellung darf nicht zum Nachteil des Betroffenen verwertet werden.

Notwendige organisatorische Maßnahmen

Für die Anlage neuer und für die Überprüfung vorhandener personenbezogener Sammlungen sowie für Verbunddateien muß der Erlaß von Errichtungsanordnungen gesetzlich vorgesehen werden, die Regelungen enthalten über

1. die Bezeichnung, den Zweck und die Rechtsgrundlage der Sammlung,
2. den in die Sammlung aufzunehmenden Personenkreis,
3. die Art und den Umfang der zu speichernden Informationen, die der Erschließung dienen können,
4. die Übermittlung von Informationen,
5. die Dauer der Aufbewahrung der Informationen und
6. die zuständige Stelle für die Anlage und Führung von Sammlungen.

Diese Errichtungsanordnungen sind zu veröffentlichen.

Daten, die zur Vorgangsverwaltung oder nur zum Nachweis polizeilichen Handelns geführt werden, sind von Datensammlungen zur Gefahrenabwehr und Strafverfolgung zu trennen."

Änderung des Musterentwurfs

Das Bayer. Staatsministerum des Innern hat mir den Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder, Stand: 8.2.1985, zur Stellungnahme überlassen. Ich begrüße, daß der Vorentwurf in einigen Bereichen bereits den Grundsätzen der Entscheidung des Bundesverfassungsgerichtes Rechnung trägt und neuere Entwicklungen des Datenschutzrechts berücksichtigen will. Ich halte den Entwurf insoweit für eine brauchbare Basis. Allerdings muß noch über eine Reihe von z.T. wesentlichen Verbesserungen der datenschutzrechtlichen Position der Bürger nachgedacht werden. Die Schwerpunkte notwendiger Änderungen betreffen insbesondere die vorbeugende Verbrechensbekämpfung, die polizeiliche Beobachtung, eine deutlichere Zweckbindung der Daten, eine gezielte Regelung bezüglich des Einsatzes automatisierter Verfahren und Fragen des Datenabgleichs. Kritisch wird zu beobachten sein, inwieweit die ebenfalls anstehenden Novellierungen zum Verfassungsschutzrecht und zur Zusammenarbeit der verschiedenen Sicherheitsbehörden zu einer verfassungsrechtlich bedenklichen Aufhebung der Trennung von Polizei und Verfassungsschutz führen. Auf Einzelheiten des Vorentwurfs, der wohl noch viele Änderungen erfahren wird, sei hier nicht eingegangen.

Derzeit enthält der Musterentwurf eines einheitlichen Polizeigesetzes Regelungsvorschläge für

- die Datenerhebung im Bereich der Gefahrenabwehr, einschließlich der vorbeugenden Bekämpfung von Straftaten,
- besondere Formen der Datenerhebung, wie polizeiliche Beobachtung, den Einsatz technischer Hilfsmittel mit besonderer Eingriffsqualität,

- die Datenspeicherung,
- den Datenabgleich und die Rasterfahndung,
- die Datenübermittlungen, wobei die Regelung hinsichtlich der Übermittlung innerhalb der Polizei und von der Polizei an andere Stellen sowie für die Datenübermittlung von anderen Behörden und Stellen an die Polizei unterscheidet,
- die Löschung von Daten (Auskunft ?) und
- die Auskunft an den Betroffenen.

5.8. Polizeilicher Staatsschutz

5.8.1. Führung der Vorgänge

Im Berichtszeitraum habe ich bei 5 Staatsschutzkommissariaten der Polizei kurze datenschutzrechtliche Prüfungen durchgeführt. Meine Stichproben haben ergeben, daß bei den Staatsschutzkommissariaten teilweise Daten notiert und Vorgänge verwahrt werden, die für die polizeiliche Aufgabenerfüllung in diesem Bereich nicht erforderlich sind. So waren u.a. Sachverhalte personenbezogen verkartet, deren Informationsgehalt für die Aufgabenerfüllung vielfach unbedeutend oder deren Sachbearbeitung lediglich administrativer Art war.

- So war beispielsweise bei einem Staatsschutzkommissariat für eine Person eine eigene Karteikarte lediglich aufgrund der Tatsache angelegt worden, daß sie zusammen mit „Hausbesetzern" eine Gastwirtschaft betreibt. Anhaltspunkte für eine sonstige auch nur irgendwie relevante Betätigung dieser Person haben sich nicht gefunden.

  Bei einem anderen Staatsschutzkommissariat wurde ein Vorgang gefunden, bei dem im Jahr 1978 eine andere Polizeidienststelle eine Erkenntnisanfrage über zwei Personen an dieses Kommissariat gerichtet hatte. Die darauf erfolgte Erkenntnismitteilung endete mit dem Satz, daß die beiden Personen weder in kriminalpolizeilicher noch in staatsschutzmäßiger Hinsicht aufgetreten seien. Auch im übrigen lagen, wie die sonstigen Unterlagen ergeben haben, keinerlei Erkenntnisse gegen diese Personen vor. Gleichwohl liegt diese negative Erkenntnismitteilung seit dem Jahr 1978 personenbezogen zugänglich in den betreffenden Akten.

- Auch in weiteren Fällen habe ich die personenbezogene Verkartung von Erkenntnisanfragen, von Personen aus der sog. Staatsschutzlage, die keinen Bezug zur speichernden Stelle haben, oder von Funktionsträgern von Ausländervereinen festgestellt, obwohl sich weder diese Personen noch die Vereine erkennbar in einer für die Aufgabenerfüllung des Staatsschutzes relevanten Weise betätigt hatten.

Ich vertrete die Auffassung, daß die Informationen, die von den Staatsschutzkommissariaten verarbeitet werden, vor ihrer personenbezogenen Erfassung und Speicherung oder gar Übermittlung wegen ihrer erhöhten Sensibilität einer weitaus kritischeren Prüfung zu unterziehen sind, als dies bei der Erfassung sonstiger polizeilicher Vorgänge notwendig ist.

Eine sachgerechte Aussonderung der von den Staatsschutzkommissariaten verwahrten Unterlagen ist im übrigen anhand der Suchkarteien meist nicht möglich. Auf den Karten sind weder Anlage- noch Wiedervorlagedaten vermerkt. Eine kontinuierliche Überprüfung der Vorgänge ist aber gerade wegen der sensiblen Informationen unbedingt erforderlich, ebenso eine flexible, dem Einzelfall gerecht werdende Handhabe von Wiedervorlagefristen. So haben Stichproben auch tatsächlich ergeben, daß längst auszusondernde Vorgänge noch personenbezogen aufbewahrt werden. Im übrigen sind auch Sachakten, die personenbezogen auswertbare Daten enthalten, einer Überprüfung auf eine eventuell notwendige Aussonderung zu unterziehen.

An einer auf das erforderliche Maß reduzierten Datenverarbeitung bei den Staatsschutzkommissariaten ist mir auch deswegen im Interesse der Bürger sehr gelegen, weil schon aus der Natur der Sache eine vergleichsweise enge Beziehung zwischen diesen Kommissariaten und dem Verfassungsschutz besteht.

5.8.2. Informationsaustausch

Übermittlungen und Speicherungen personenbezogener Daten im Zusammenhang mit der Blockade einer Kaserne habe ich stichprobenartig einer Überprüfung unterzogen. Dabei habe ich auch Verfahrensweisen bei der Verarbeitung personenbezogener Daten festgestellt, die unabhängig von diesem Einzelvorgang offenbar Übung bei Staatsschutzdienststellen sind. Weil diese Vorgänge teilweise einer gewissen Geheimhaltung unterliegen, ist es es mir versagt, Einzelheiten meiner Ermittlungen mitzuteilen. Ganz allgemein ist zu bemerken, daß mich die Ergebnisse der Stichproben teilweise nachdenklich gestimmt haben. Auch diese Ermittlungen haben meinen Eindruck verstärkt, daß im Staatsschutzbereich Speicherungen und Datenübermittlungen aufgrund der bestehenden Richtlinien vorgenommen werden, die zum Teil zur Aufgabenerfüllung der speichernden Stellen nicht in diesem Umfang erforderlich sind. Dabei gebe ich zu bedenken, daß die Fälle jeweils für sich allein betrachtet nicht sehr bedeutsam erscheinen, für den einzelnen Betroffenen jedoch sehr wichtig sein können.

- Die zuständige Polizeidienststelle hat eine Liste von mehr als 300 Personen, gegen die Ermittlungsverfahren wegen Nötigung eingeleitet worden sind, an das Bundeskriminalamt und an das Bayer. Landeskriminalamt (LKA) mit der Bitte „um Mitteilung vorliegender Erkenntnisse" versandt. Das LKA hat zu den Personen aus der Liste, zu denen ihm jeweils Erkenntnisse vorgelegen haben, an zahlreiche andere Polizeidienststellen Daten übermittelt, die bis dahin offenbar mit der Sachbearbeitung der zugrundeliegenden Strafverfahren nicht befaßt waren. Hierbei wurden auch Daten übermittelt, die nicht auf staatsschutzrelevante Vorgänge zu beziehen waren. In diesem Zusammenhang ist aufgefallen, daß das Bundeskriminalamt dem Bayer. Landeskriminalamt bayerische Erkenntnisse mitgeteilt hat, die dem Bayer. Landeskriminalamt nicht bekannt waren. Offensichtlich hatte das Bayer. Landeskriminalamt als zuständige bayerische Zentralstelle eine Verkartung oder die Anlage von Personalakten zum Zeitpunkt der Kenntnis dieser Vorgänge für nicht erforderlich gehalten.

- Das LKA hat infolge eines über die Grenzen der Bundesländer hinausgehenden Nachrichtenaustausches auch Akten über Personen angelegt, gegen die in Bayern kein Ermittlungsverfahren geführt worden war und die in Bayern weder geboren noch wohnhaft sind. Ich habe Zweifel, ob eine solche Speicherung personenbezogener Daten, die keinen Bezug zu Bayern und damit zum LKA aufweisen, erforderlich ist. Das LKA hat auf entsprechende Anfragen diese nur außerbayerischen Erkenntnisse wieder über die Landesgrenzen hinweg anderen Kriminalämtern mitgeteilt. Wegen der Zweifel an der Zulässigkeit der Speicherung solcher personenbezogener Daten ergeben sich auch Bedenken hinsichtlich der Zulässigkeit derartiger Datenübermittlungen.

  Das Landeskriminalamt eines anderen Bundeslandes hat an das BLKA jeweils dann Erkenntnisse mitgeteilt, wenn ein Bürger aus dem dortigen Zuständigkeitsbereich nach Bayern umgezogen ist. Die Tatsache des Umzuges von einem Bundesland in das andere allein kann m. E. eine derartige Datenübermittlung grundsätzlich nicht rechtfertigen. Das LKA hat auf solche Weise erlangte Daten an das Bayer. Landesamt für Verfassungsschutz und an die jeweilige neue bayerische Wohnsitzdienststelle weitergemeldet. Gegen eine solche Praxis bestehen grundsätzlich datenschutzrechtliche Bedenken.

- Das LKA hat in einem Sammelfernschreiben an mehrere Polizeidienststellen allgemeine, nicht staatsschutzbezogene Erkenntnisse mitgeteilt. So hat das BKA z.B. mitgeteilt, daß ein Betroffener, gegen den im übrigen keine Erkenntnisse vorliegen, vor Jahren seinen Paß in Istanbul verloren hat. Ich habe Bedenken, ob die Übermittlung solcher Sachverhalte zwischen Staatsschutzdienststellen im konkreten Fall wirklich erforderlich war.

  Muß in diesem Sammelfernschreiben, das mehrere Landeskriminalämter erreicht, auch mitgeteilt werden, daß von einigen der Personen – wohl als einzige vorliegende Information – die Tatsache bekannt sei, daß sie Teilnehmer an einer unangemeldeten Versammlung anläßlich eines Bundeswehrstandortballes gewesen seien? Ich habe diesbezüglich erhebliche Zweifel. Personen, die im Wege eines solchen Sammelfernschreibens dem Bundeskriminalamt bekannt wurden, sind zudem dort in das System NADIS eingestellt worden.

  Im Wege eines kriminalpolizeilichen Meldedienstes in Staatsschutzangelegenheiten wurden in größerer Zahl Delikte, wie Sachbeschädigungen, Nötigungen und Farbschmierereien übermittelt. Solche Delikte werden im Einzelfall unter die Meldedienstrichtlinien für den Staatsschutz eingeordnet. Meines Erachtens zeigt dies, daß diese Richtlinien konkretisiert werden sollten, damit der Staatsschutzbezug stärker herausgestellt wird.

Meines Erachtens kann aus diesem Fall der Schluß gezogen werden, daß Sicherheitsbehörden wegen zu wenig präziser Richtlinien hier nicht immer so handeln, wie es auch die weiten Teile der Bevölkerung erwarten, die als loyale Staatsbürger das Recht und die Pflicht des Staates respektieren, die für eine effektive Verbrechensbekämpfung notwendigen Informationen zu beschaffen, ohne nicht oder nur am Rande Betroffene zu belasten. Dazu gehört jedoch auch, schwere Taten oder Gefährdungen mit höherem Einsatz, leichteren Fällen mit entsprechend geringerem zu begegnen und Unbeteiligte nicht mehr als nötig zu belasten. Das macht aber deutlich, daß auch im Staatsschutzbereich die bisherigen Meldedienste und Erkenntnisanfragen einer kritischen Überprüfung unterzogen werden müßten. Diese Überprüfung erscheint mir nicht zuletzt deshalb dringlich zu sein, weil mit der Einführung des Informationssystems APIS (siehe dort) diese breit gestreuten, jedoch nicht immer sehr wichtigen Informationen bundesweit im direkten Abruf zur Verfügung gestellt werden sollen.

5.8.3. Errichtung einer Arbeitsdatei PIOS – Innere Sicherheit (APIS)

Beabsichtigt die Polizei neue automatisierte Verfahren einzuführen, so hat sie mehr noch als bisher zu prüfen, wie dieses Automationsvorhaben sich auf bisher bestehende Datensammlungen und Meldedienste auswirkt. Mehrfachspeicherungen, neue Zugriffsmöglichkeiten, vermehrte Übermittlungswege und neue Möglichkeiten der Zusammenführung von personenbezogenen Daten können im Einzelfall die Rechte der Bürger unverhältnismäßig beeinträchtigen.

Unter diesem Gesichtspunkt habe ich gegen die zunächst für Sommer dieses Jahres beabsichtigte Einführung einer neuen Arbeitsdatei „APIS" Bedenken angemeldet. Meines Erachtens können beim Betrieb der APIS-Datei in der vorgesehenen Form neue Probleme entstehen, weil bisher getrennte Datenbestände zur Terrorismusbekämpfung und zum polizeilichen Staatsschutz, der von seiner Zuständigkeit auch viele Taten von vergleichsweise geringfügiger Bedeutung zu verfolgen hat, zusammengeführt werden sollen. Auch werden durch diesen Einsatz des PIOS-Verfahrens im Staatsschutzbereich erheblich erweiterte Möglichkeiten der Aktenerschließung einschließlich der Möglichkeit zur Speicherung „anderer Personen" eröffnet. Das Problem der Zusammenführung von Daten aus Terrorismus und Staatsschutz verschärft sich noch dadurch, daß eine klare Abgrenzung fehlt, welche Straftaten dem polizeilichen Staatsschutz zuzuordnen sind. Teilweise verfolgt der polizeiliche Staatsschutz auch alle jene Straftaten, die im weitesten Sinne einen Zusammenhang mit politischen Themen haben könnten. Darunter fallen auch Vergehen nach dem Versammlungsgesetz, Sachbeschädigungen wie z.B. Farbschmierereien, Hausfriedensbruch, Beleidigungen und Nötigungen. Ich verkenne nicht, daß möglicherweise unter polizeilichen Gesichtspunkten auch dieser Personenkreis zu erfassen ist. Jedoch halte ich es nicht für erforderlich, diese Personen zusammen mit Straftätern, die unter Terrorismusverdacht stehen oder schwerer Staatsschutzdelikte bezichtigt werden, in einer Datei zu speichern. Denn es ist nicht auszuschließen, daß allein die Tatsache einer Speicherung in APIS durch einen nicht völlig auszuschließenden unkritischen Gebrauch der Dateibenutzer zu unverhältnismäßigen Nachteilen für den Betroffenen führen kann.

Im bisherigen Stand des beabsichtigten Verfahrens vermisse ich auch eine klare Regelung, was mit den bisherigen Meldediensten im Staatsschutzbereich geschieht und in welchem Verhältnis diese zu dem Verfahren APIS stehen werden. Mehrfachspeicherungen oder Mehrfachübermittlungen sollten jedenfalls in diesem besonders sensiblen Bereich vermieden werden. Entsprechende, noch zu schaffende, Regelungen müssen diesem Problem gerade

im Hinblick auf den weiterhin praktizierten Informationsaustausch konventioneller Art vorbeugen. Im übrigen müßte sichergestellt werden, daß Daten, die in einem Ausnahmefall doppelt in verschiedenen Dateien gespeichert werden müssen, nicht nach verschiedenen Kriterien gelöscht werden.

Der Grundsatz der Zweckbindung ist gerade bei einer solchen Datei wie APIS besonders wichtig. So muß eine Verwendung der Daten für andere Zwecke als der Bekämpfung des Terrorismus und der Staatsschutzkriminalität ausgeschlossen sein. Auskünfte aus einer solchen Datei müssen also – anders als dies für andere polizeiliche Dateien gelten mag – nur auf einen ganz engen Personenkreis beschränkt bleiben.

6. Verfassungsschutz

6.1. Prüftätigkeit beim Bayer. Landesamt für Verfassungsschutz

Wie bereits in den vergangenen Jahren hat sich meine Prüftätigkeit beim Bayer. Landesamt für Verfassungsschutz auf zwei Bereiche gestützt:

Soweit Bürger sich mit Eingaben an mich wenden, in denen sie die Befürchtung äußern, daß beim Verfassungsschutz möglicherweise unrichtige Daten gespeichert werden, gehe ich diesen Einzelfällen nach. Soweit erforderlich, nehme ich hier auch Einblick in die zugrundeliegenden Personen- und Sachakten. Die Zahl dieser Bürgereingaben hat im Berichtszeitraum im Vergleich zu früheren Jahren leicht abgenommen.

Daneben habe ich auch in diesem Berichtszeitraum das Landesamt für Verfassungsschutz zu einer kurzen generellen Prüfung aufgesucht. Ziel dieser kurzen Prüfung war es, einige grundsätzliche Erkenntnisse über die Praxis bei NADIS-Eintragungen, die Führung der diesen Eintragungen zugrundeliegenden Akten und die Handhabung von Datenübermittlungen zum und vom Landesamt für Verfassungsschutz nachzuvollziehen. Damit soll die Datenverarbeitung gegebenenfalls grundsätzlich auf Schwachstellen geprüft werden, die aus datenschutzrechtlicher Sicht zu rügen wären.

Im folgenden nun einige Ergebnisse der Prüfungen:

Bei Speicherungen in NADIS habe ich festgestellt, daß das auch für die Aussonderung wesentliche Eintragungsdatum in einigen Fällen nicht auf den Tag der letzten Erkenntnisse, sondern auf den um einen nicht unwesentlichen Zeitraum verzögerten Abschluß der Sachbearbeitung bezogen war. Auch führten Änderungen von Wohnanschriften oder die bloße Bearbeitung von Erkenntnisanfragen – ohne daß sich hieraus besondere Erkenntnisse ergeben hätten – zu einer Neufestsetzung dieses Datums. Dies bewirkte automatisch eine Verlängerung der Aussonderungsfrist. Eine Fristberechnung, die auf solcher Sachbehandlung beruht, ist grundsätzlich nicht sachgerecht. Das Landesamt für Verfassungsschutz hat dieser Beanstandung bereits Rechnung getragen.

Meines Erachtens darf das System NADIS auch nicht dazu dienen, einen Nachweis für sämtliche Verwaltungstätigkeiten des Landesamtes für Verfassungsschutz darzustellen. Solches kann nur im Rahmen eines Registratur- oder Vorgangsverwaltungssystems festgehalten werden. Bearbeitete Verwaltungsanfragen, die keine besonderen Erkenntnisse ergeben haben, sollten daher grundsätzlich nicht in NADIS eingespeichert werden. Das Landesamt für Verfassungsschutz wird diese Frage überprüfen.

Bei der erstmaligen Anlage eines Personenaktes muß besonders intensiv geprüft werden, ob die Voraussetzungen für eine solche Speicherung gegeben sind. Meines Erachtens muß sich auch aus dem Akt entnehmen lassen, daß diese Prüfung tatsächlich stattgefunden hat. Liegt nämlich einmal ein Akt vor, werden auch Vorgänge zu diesem Akt genommen, die andernfalls nicht personenbezogen aufbewahrt worden wären.

Die im System NADIS eingetragenen Daten müssen sich aus den genannten Akten eindeutig und einwandfrei entnehmen lassen. Eines der Ziele des Datenschutzes liegt darin, daß selbst bei einer einfachen und unaufwendigen Sachbearbeitung der Zugriff auf vollständige und richtige Daten zu einer Person gesichert ist. Werden jedoch zu einer Person auf verschiedenen Datenträgern, die an verschiedenen Stellen gelagert sind, Daten geführt, besteht das Risiko, daß bei schnellem Zugriff auf die Daten wegen der dann nicht auszuschließenden Unvollständigkeit möglicherweise ein unrichtiger Eindruck über den Betroffenen entsteht. Auch ist durch eine eindeutige und übersichtliche Führung der Daten sicherzustellen, daß die Daten nicht unterschiedliche Aktualität besitzen, denn auch dies könnte im Einzelfall zu unrichtigen Schlußfolgerungen führen. Ich habe daher beim Landesamt für Verfassungsschutz darauf hingewiesen, daß die Informationsspeicherung übersichtlicher und für den Sachbearbeiter einwandfrei nachvollziehbar erfolgen muß. Hierzu habe ich einige Anregungen in organisatorischer Hinsicht gegeben.

Bei der kurzen Prüfung beim Landesamt für Verfassungsschutz bin ich noch auf weitere Probleme gestoßen:

So habe ich einem Vorgang entnommen, daß offensichtlich im universitären Bereich eine Kandidatenliste einer nicht extremistischen Studentenorganisationen unkritisch in einem Akt aufgenommen worden ist, ohne daß Anhaltspunkte vorlagen, die ein Tätigwerden des Landesamt für Verfassungsschutz erfordert hätten. Diese Unterlagen hätten sofort nach Eingang beim Landesamt für Verfassungsschutz vernichtet werden müssen. Die Unterlagen wurden inzwischen vernichtet; das Landesamt erklärte, die Unterlagen seien zu keinem Zeitpunkt organisations- oder personenbezogen ausgewertet worden oder gespeichert gewesen.

Personenakten und zugehörige NADIS-Einträge dürfen nur hinsichtlich der Personen angelegt werden, die tatsächlich in ihrer Person Anlaß für eine Speicherung beim Landesamt für Verfassungsschutz geben. Wird statt der Person, der eine für das Landesamt für Verfassungsschutz relevante Tätigkeit vorgeworfen wird, der Hinweisgeber (Zeuge) gespeichert, kann dies Anlaß zu Mißverständnissen sein. Der Vorgang ist nun gelöscht.

Überhaupt sollte das Landesamt für Verfassungsschutz darauf hinwirken, daß die Stellen, von denen regelmäßig Meldungen eingehen, sich auf die Übermittlung solcher Informationen beschränken, die den Aufgabenbereich des

Landesamtes für Verfassungsschutz, tatsächlich berühren. Gelangen gleichwohl unbedeutende Meldungen in den Bereich des Landesamtes für Verfassungsschutz, dürfen diese nicht aufbewahrt werden. So ist beispielsweise von einem Staatsschutzkommissariat mitgeteilt worden, wer als Fachvortragender zu einem ökologischen Thema in einer Kleinstadt gesprochen hat. Diese Mitteilung war vom Landesamt für Verfassungsschutz noch nicht ausgewertet und ist nun nicht mehr gespeichert.

Bezüglich der Aussonderung bestehen beim Landesamt für Verfassungsschutz, wie dies aus anderen Bereichen auch bekannt ist, sogenannte Regelfristen. Die Ansicht des Landesamtes für Verfassungsschutz, daß die vorgegebenen Regelfristen den Sachbearbeiter von einer weiteren einzelfallbezogenen Prüfung der Fristsetzung entbinden, kann ich nicht teilen. Auch beim Verfassungsschutz können Regelfristen nur als Anhaltspunkt dienen. Im konkreten Einzelfall muß aber je nach Erforderlichkeit von dieser Frist nach unten oder ggf. auch nach oben abgewichen werden. Andernfalls käme die diesbezügliche Sachbearbeitung einem reinen Automatismus gleich, der gerade wegen der Sensibilität der beim Verfassungsschutz vorgehaltenen Daten besonders problematisch wäre. Nach meinen Feststellungen werden Vorgänge unterschiedlicher Bedeutung durch die starre Fristensetzung gleichbehandelt. Somit wird gegen den Gleichheitsgrundsatz verstoßen, wenn weniger bedeutsame Ereignisse hinsichtlich der Speicherungsdauer mit schweren Fällen gleichbehandelt werden. Derartige Speicherungen können im Einzelfall unzulässig werden. Auch hierzu habe ich Anregungen für eine flexiblere Handhabung der Fristensetzung gegeben. Das Landesamt für Verfassungsschutz hat inzwischen entsprechende, detaillierte Richtlinien in Bearbeitung.

Bei Datenübermittlungen habe ich festgestellt, daß Aufgabe und Beantwortung von Fernschreiben zu automatisch abgewickelt werden. Offensichtlich wird der Empfängerkreis der Anfrage vom Landesamt für Verfassungsschutz stets mit der Antwort versorgt. Auf diese Weise können Stellen Erkenntnisse des Verfassungsschutzes erfahren, die für ihre Aufgabenerfüllung nicht erforderlich sind.

Ich bin mir bewußt, daß eine kurze Prüfung in einem der Öffentlichkeit weitgehend verschlossenen Bereich nur punktuelle datenschutzrechtliche Erkenntnisse gewinnen läßt. Nach dem Bayer. Datenschutzgesetz ist für die Einhaltung des Datenschutzes bei den einzelnen Behörden nicht der Landesbeauftragte für den Datenschutz verantwortlich. Diese Verantwortung liegt bei der jeweiligen Behörde. Gegebenenfalls ist im Wege der Fachaufsicht ein ordnungsgemäßer Vollzug auch des Datenschutzrechts sicherzustellen. Auch hier Anregungen zu geben, ist Zweck meiner Tätigkeit.

6.2. Sicherheitsüberprüfungen und der Fall N.

Personen, die bei der öffentlichen Verwaltung tätig oder in der Privatwirtschaft beschäftigt sind, werden einer Sicherheitsüberprüfung unterzogen, soweit ihnen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Kenntnisse anvertraut werden, sie Zugang dazu erhalten sollen oder ihn sich verschaffen können. Mit der Durchführung derartiger Sicherheitsüberprüfungen sind u.a. die Verfassungsschutzbehörden des Bundes und der Länder betraut. In Bayern wirkt das Bayer. Landesamt für Verfassungsschutz an Sicherheitsüberprüfungen mit.

Von dieser gesetzlichen Aufgabenzuweisung der Mitwirkung durch das Landesamt für Verfassungsschutz abgesehen, fehlen präzise gesetzliche Regelungen für die Durchführung der Sicherheitsüberprüfungen. Derzeit bestehen im wesentlichen nur entsprechende Richtlinien. Weil die Sicherheitsermittlungen zum Teil sehr intensiv in den privaten durch Art. 2 Abs. 1 und Art. 1 Abs. 1 Grundgesetz geschützten Lebensbereich eindringen und sehr sensible personenbezogene Daten gespeichert werden, die das Grundrecht auf informationelle Selbstbestimmung berühren, bedürfen die Sicherheitsüberprüfungen einer eigenen gesetzlichen Regelung. Dies gilt auch, soweit nach Abschluß der Sicherheitsüberprüfung das Grundrecht auf Freizügigkeit eingeschränkt wird.

Festzulegen sind hierbei der Verfahrensablauf, die am Verfahren beteiligten Behörden, die notwendigen Datenübermittlungen und der Umfang der als Ergebnis der Überprüfung zu speichernden Daten. Die Überprüfungen sind auf das tatsächlich erforderliche Maß zu beschränken. Dies gilt sowohl hinsichtlich der Zahl der zu überprüfenden Personen, wie hinsichtlich der Intensität der Prüfung, die von der Gefährdung oder dem Risiko im Einzelfall abhängen muß. Hierbei ist der Grundsatz der Verhältnismäßigkeit zu achten.

Die Sicherheitsüberprüfung darf auch erst dann durchgeführt werden, wenn die sonstigen Voraussetzungen zur Befassung mit sicherheitsrelevanten Vorgängen oder zum Einsatz im sicherheitsrelevanten Bereich gegeben sind. Bezüglich des personellen Sabotage-Schutzes ist zudem die exakte Beschreibung der sicherheitsempfindlichen Bereiche und die Begrenzung der Prüfung auf tatsächlich in diesem Bereich eingesetzte Personen zu fordern.

Das Verfahren muß für den Betroffenen transparent sein. Er ist über die Tatsache, den Ablauf und das Ergebnis der Sicherheitsprüfung zu unterrichten. Ihm ist Gelegenheit zur Stellungnahme zu geben, insbesondere zu den Auskünften sog. „Referenzpersonen". Die Ausnahmen von der Unterrichtungspflicht sind sehr eng zu fassen. Auch die Art und Weise der Durchführung der Sicherheitsüberprüfung darf den Betroffenen nicht unverhältnismäßig belasten. So sollen beispielsweise die befragten Referenzpersonen über den Zweck ihrer Befragung unterrichtet werden, damit sie nicht Fehlschlüsse zu Lasten des Betroffenen ziehen.

Soweit im Rahmen der Sicherheitsüberprüfung auch Nachforschungen über Dritte angestellt werden sollen, z.B. über Ehegatten, sonstige Angehörige, Verlobte, in eheähnlicher Gemeinschaft Lebende oder Auskunftspersonen, ist grundsätzlich deren Einwilligung einzuholen. Die Speicherung von Daten über diese Personen ist auf ein Minimum zu beschränken und darf grundsätzlich nicht personenbezogen erschließbar sein.

Soweit die Verfassungsschutzbehörden in diesen Verfahren Erkenntnisse von der Polizei erholen, wird zu prüfen sein, ob künftig polizeiliche und nachrichtendienstliche Ermittlungen stärker zu trennen sind. So sollte es nicht Aufgabe des Verfassungsschutzes sein, im Rahmen der Sicherheitsüberprüfung die Auskünfte aller beteiligten Stellen zu koordinieren.

Die im Zusammenhang mit der Sicherheitsüberprüfung angefallenen personenbezogenen Daten dürfen in der Regel nur für diesen Zweck verwendet werden. Diese Daten sind grundsätzlich von den sonstigen beim Verfassungsschutz vorgehaltenen Vorgängen zu trennen.

Schließlich ist sicherzustellen, daß die Verfahrensregelungen nicht durch andere Formen und Wege der Sicherheitsüberprüfungen unterlaufen werden.

Beispiel einer unzulässigen Sicherheitsüberprüfung (der Fall N.)

Ein Petent hat sich mit einer Eingabe an mich gewandt, weil er – wie sich herausstellte zu Recht – befürchtete, daß ihm durch fehlerhafte Datenübermittlungen im Rahmen von Sicherheitsüberprüfungen Nachteile entstanden sein könnten. Der Petent war ab Ende letzten Jahres im Rahmen eines Dienstvertrages als Programmierer bei einer Firma beschäftigt, die auch in sicherheitsempfindlichen Bereichen aktiv ist. Zu Beginn seiner Tätigkeit hat der Petent einer Sicherheitsüberprüfung durch diese Firma zugestimmt. Diese Firma hat dann über den Petenten beim Bayer. Landesamt für Verfassungsschutz angefragt. Dort wurde festgestellt, daß der Petent nicht in NADIS gespeichert ist und keine sonstigen Erkenntnisse über ihn vorliegen. Das Landesamt für Verfassungsschutz hat daneben bei der für den Wohnsitz des Petenten zuständigen Polizeibehörde Auskünfte polizeilicher Art über den Petenten angefordert. Die Polizeidienststelle hat mitgeteilt, daß gegen den Petenten 1983 ein Ermittlungsverfahren wegen Hausfriedensbruchs und Beleidigung geführt und nach § 153 a Strafprozeßordnung eingestellt worden sei und außerdem im Herbst 1984 ein Ermittlungsverfahren wegen Körperverletzung und Beleidigung eingeleitet worden sei.

Allein aufgrund der Mitteilung, daß derzeit ein Ermittlungsverfahren anhängig ist, hat das Landesamt für Verfassungsschutz gegenüber der Beschäftigungsfirma das Votum abgegeben, daß derzeit gegen den Petenten in sicherheitsrechtlicher Hinsicht Bedenken bestünden. Daraufhin wurde dem Petenten von der Beschäftigungsfirma unter Hinweis auf diese Sicherheitsüberprüfung die Erlaubnis zum Betreten des Werksgeländes entzogen. Nähere Auskünfte über die der Sicherheitsprüfung zugrundeliegenden Erkenntnisse hat der Petent nicht erhalten.

Meine Ermittlungen haben ergeben, daß beide von der Polizeidienststelle mitgeteilten Ermittlungsverfahren für die Tätigkeit des Landesamts für Verfassungsschutz nicht von Bedeutung waren. So ist das Verfahren wegen Hausfriedensbruch strafrechtlich nicht von Gewicht gewesen, was sich nicht zuletzt aus der Verfahrenseinstellung nach § 153 a Strafprozeßordnung ergibt. Auch der zugrundeliegende Tatbestand war ohne jede politische oder verfassungsrechtliche Bedeutung; dem Verfahren lag die Verwechslung eines Müllcontainers zugrunde.

Das Ermittlungsverfahren wegen Körperverletzung betraf einen „Tritt in das Hinterteil" des behandelnden Arztes. Bereits insoweit war ein Bezug zur Tätigkeit des Landesamtes für Verfassungsschutz nicht erkennbar. Außerdem betraf dieses Verfahren nicht den Petenten, sondern einen wesentlich lebensjüngeren Studenten ähnlichen Namens.

Somit hat auch das Landesamt für Verfassungsschutz an die Beschäftigungsfirma des Petenten unrichtige Daten übermittelt. Dies habe ich beanstandet. Das Landesamt für Verfassungsschutz hat seine Auskunft gegenüber der Beschäftigungsfirma inzwischen berichtigt. Aus datenschutzrechtlicher Sicht ist hier folgendes noch festzustellen:

Unabhängig davon, daß ein Irrtum bezüglich der Person des Betroffenen vorgelegen hat, ist es meines Erachtens bedenklich, daß das Landesamt für Verfassungsschutz sein negatives Votum, das einen Arbeitsplatzverlust zufolge haben kann, auf knappe polizeiliche Angaben stützt, ohne selbst zu prüfen, ob der tatsächliche Sachverhalt, der den Ermittlungsverfahren wegen Hausfriedensbruchs, Beleidigung und Körperverletzung zugrundeliegt, wirklich relevant ist. Eine intensivere Prüfung hätte zudem die Unrichtigkeit der Daten ergeben.

Der Fall hat erneut gezeigt, daß die Polizei an das Landesamt für Verfassungsschutz Daten übermittelt, die ohne wirkliche Bedeutung für dessen vom Gesetz zugewiesene Tätigkeit sind. Offensichtlich ist dieses von mir bereits mehrfach gegenüber dem Innenministerium angesprochene Problem bisher noch nicht gelöst worden. Schließlich hat es sich auch in diesem Fall als sehr problematisch erwiesen, daß dem Betroffenen nicht die der negativen Entscheidung des Landesamtes für Verfassungsschutz zugrundeliegenden Erkenntnisse vorgehalten worden sind. Zumindest die Personenverwechslung hätte sich bereits auf diese Weise feststellen lassen.

Bedenklich stimmt auch, daß das Landesamt für Verfassungsschutz relativ unbedeutende polizeiliche Erkenntnisse und ein laufendes Ermittlungsverfahren wegen kleiner Straftaten ohne Bezug zur Tätigkeit des Landesamtes für Verfassungsschutz genügen läßt, um ein negatives Ergebnis einer Sicherheitsüberprüfung festzustellen.

Die über diesen kurzen Bericht hinausgehende Problematik der Einschaltung des Bayer. Landesamtes für Verfassungsschutz in solche Überprüfungen muß ich an dieser Stelle unberücksichtigt lassen.

Das Bayerische Landesamt für Verfassungsschutz hat sich beim Beschwerdeführer schriftlich entschuldigt und bei der betroffenen Firma den Sachverhalt klargestellt.

6.3. Bereichsspezifischer Datenschutz bei Nachrichtendiensten

Die Bundesregierung hat auf eine große Anfrage von Abgeordneten zur „Datenverarbeitung im Sicherheitsbereich" die in der Bundestagsdrucksache 10/3035 auch zu den beabsichtigten neuen gesetzlichen Regelungen bei den Nachrichtendiensten Stellung genommen. So ist unter anderem beabsichtigt, ein neues Zusammenarbeitsgesetz für die Sicherheitsbehörden zu erlassen. In diesem Gesetz sollen, wie die Bundesregierung mitteilt, Übermittlungsvorschriften für die Zusammenarbeit

- der Nachrichtendienste untereinander, soweit gesetzliche Vorschriften noch nicht bestehen, und
- zwischen der Polizei des Bundes und der Länder und den Nachrichtendiensten

in Angelegenheiten des Staats- und Verfassungsschutzes aufgenommen werden. Dabei soll die Zulässigkeit der Übermittlung personenbezogener Daten an präzise gesetzliche Voraussetzungen gebunden werden. Dabei sei zu unterscheiden

- an welche Sicherheitsbehörden übermittelt werde (die Übermittlung innerhalb der Nachrichtendienste habe eine andere Qualität als die zwischen der Polizei und diesen Diensten),
- auf welche Art und Weise die übermittelten Daten erhoben worden sind und
- die Sensibilität der zu übermittelten Daten z.B. von G10-Erkenntnissen.

Auch für den Militärischen Abschirmdienst werde eine gesetzliche Regelung erwogen, die nach den derzeitigen Überlegungen an das Gesetz für das Bundesamt für Verfassungsschutz angelehnt sei. Inwieweit ein Gesetz für den Bundesnachrichtendienst geplant ist, vermag ich nur Pressemitteilungen zu entnehmen. Weil bayerische Behörden jedoch im gewissen Maße auch mit dem Bundesnachrichtendienst und dem Militärischen Abschirmdienst zusammenzuarbeiten haben, besteht auch aus bayerischer Sicht ein gewisses Interesse an entsprechenden Regelungen (auf Nr. 4.3.11.2 des 6. Tätigkeitsberichtes darf ich insoweit hinweisen).

Die Datenschutzbeauftragten des Bundes und der Länder haben sich gemeinsam Gedanken gemacht, welche Anforderungen an Datenschutzregelungen für den Verfassungsschutz zu stellen seien. Nach dem bisherigen Stand der Überlegungen sind aus bayerischer Sicht folgende Grundsätze zu beachten:

Wegen der Sensibilität der bei den Verfassungsschutzbehörden verarbeiteten Daten sind für deren Datenverarbeitung präzise gesetzliche Grundlagen erforderlich. Diese Datenverarbeitung ist im besonderen Maße geeignet, in das informationelle Selbstbestimmungsrecht der Bürger einzugreifen. Zudem findet sie fast vollständig im Geheimen statt und ist daher der Kontrolle durch die Öffentlichkeit wie durch den Betroffenen selbst weitgehend entzogen. Dabei bin ich mir selbstverständlich der Tatsache bewußt, daß wegen der Art der Tätigkeit der Verfassungsschutzbehörden an die Transparenz der Vorschriften auch keine übertriebenen Anforderungen gestellt werden dürfen. Andererseits muß auch der Verfassungsschutz in einem demokratischen Rechtsstaat gerade auch wegen der notwendigen Vertrauensbildung gegenüber den Bürgern seine Tätigkeit auf einer möglichst präzisen gesetzlichen Grundlage ausüben. Weil über die Datenverarbeitung im Einzelfall meist nichts bekannt wird, ist es für den Bürger von besonderer Bedeutung, daß er wenigsten den gesetzlichen Bestimmungen entnehmen kann, aus welchem Anlaß, in welcher Form und zu welchem Zweck der Verfassungsschutz Daten über ihn verarbeiten darf. Die Regelung muß auch in sich differenziert sein und auf die unterschiedlichen Aufgaben der Verfassungsschutzbehörden abgestellt werden. Was beispielsweise an Maßnahmen für die konkrete Abwehr von Spionen notwendig sein kann, ist nicht gleichzeitig auch für die Mitwirkung an Sicherheitsüberprüfungen angemessen.

Weil sich durch den zunehmenden Einsatz der elektronischen Datenverarbeitung in allen Lebensbereichen auch beim Verfassungsschutz manche Risiken für den Bürger verstärkt haben, kann es beim Verfassungsschutz nicht allein darum gehen, die derzeitige Praxis unbesehen gesetzlich festzuschreiben. Vielmehr muß der Umfang zulässiger Informationsverarbeitung der Verfassungsschutzbehörden durch spezielle Aufgaben- und Befugnisnormen dem Grundsatz der Verhältnismäßigkeit und insbesondere neben den anderen Grundrechten auch dem informationelle Selbstbestimmungsrecht Rechnung tragen. Hierbei sind inbesondere auch die in den letzten Jahren ergangenen Entscheidungen des Bundesverfassungsgerichts zu berücksichtigen, zuletzt die im Juli dieses Jahres ergangene Entscheidung zum Demonstrationsrecht.

Die Regelung muß grundsätzlich sämtliche Formen der Verarbeitung personenbezogener Daten erfassen, muß den Grundsatz der Zweckbindung berücksichtigen und auch den Grad der im Einzelfall zulässigen Automatisierung feststellen. Ebenso müssen die Grenzen für Art und Umfang der im Einzelfall einzusetzenden nachrichtendienstlichen Mitteln festgelegt werden, soweit dies der Natur dieser Sache nach möglich ist.

Da mir das Bayer. Staatsministerium des Innern den Entwurf des Zusammenarbeitsgesetzes zur Stellungnahme vorgelegt hat, habe ich diese Anforderungen auch gegenüber dem Bayer. Staatsministerium des Innern geltend gemacht. Dabei ist deutlich geworden, daß der derzeit vorliegende Entwurf aus datenschutzrechtlicher Sicht einer weiteren Überarbeitung bedarf.

6.4. Auskunftsanspruch gegenüber Verfassungsschutzbehörden

Nach Art. 8 Abs. 2 Nr. 5 Bayer. Datenschutzgesetz besteht kein Auskunftsanspruch gegenüber Verfassungsschutzbehörden. Ich vertrete hierzu die Auffassung, daß eine solche Versagung der Auskunft vom Landesamt für Verfassungsschutz eine auf den Einzelfall bezogene Ermessensentscheidung ist. In der Rechtssprechung ist diese Auffassung jedoch nicht unumstritten. Zwar wird diese Ansicht von einer Reihe von Gerichten vertreten, jedoch hat der Bayer. Verwaltungsgerichtshof mit Urteil vom 24.3.1983 entschieden, daß der Betroffene keinen Anspruch auf eine ermessenfehlerfreie Entscheidung in den Fällen des Art. 8 Abs. 2 Bayer. Datenschutzgesetz hat.

Weil diese Angelegenheit strittig ist, kommt der Prüftätigkeit durch den Bayer. Landesbeauftragten für den Datenschutz bei den Verfassungsschutzbehörden besonderes Gewicht zu. Wenn der Bürger schon selbst keine Auskunft über eventuell beim Verfassungsschutz gespeicherte Daten bekommt, muß ihm zumindest die Möglichkeit offenstehen, durch Anrufung des Landesbeauftragten für den Datenschutz die Ordnungsgemäßheit einer eventuellen Speicherung bei diesem Amt feststellen zu lassen. Das Bundesverfassungsgericht hat in der Entscheidung zum Volkszählungsgesetz festgestellt, daß mit dem Recht auf informationelle Selbstbestimmung eine Rechtsordnung nicht vereinbar wäre, „in der Bürger nicht mehr wissen können, wer, was, wann und bei welcher Gelegenheit über sie weiß" und in der Bürger unsicher wären, „ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft

gespeichert, verwendet oder weitergeben werden". Wenn schon der Bürger nicht selbst wissen kann, ob und ggf. welche Daten der Verfassungsschutz über ihn gespeichert hat, kann zumindest die diesbezüglich umfassende Prüftätigkeit des Landesbeauftragten für den Datenschutz einen gewissen Ausgleich darstellen. Andernfalls wäre das Grundrecht auf informationelle Selbstbestimmung gegenüber dem Verfassungsschutz völlig seiner Grundlage entzogen.

Stellt ein Bürger einen Auskunftsantrag beim Landesamt für Verfassungsschutz, ist dieser auch im Hinblick auf die Geltendmachung des grundrechtlich verbürgten Rechts auf informationelle Selbstbestimmung zu sehen. Dies bedeutet jedoch auch, daß der Bürger nicht durch Registrierungen seines Auskunftsbegehrens möglicherweise von der Wahrnehmung dieses Rechts abgehalten wird. Ähnlich hat sich das Bundesverfassungsgericht zuletzt in seiner Entscheidung zum Demonstrationsrecht geäußert. Bezüglich der Zeitdauer der Aufbewahrung von entsprechenden Auskunftsanträgen der Bürger beim Bayer. Landesamt für Verfassungsschutz stehe ich mit dem Bayer. Staatsministerium des Innern in Verhandlungen.

7. Justiz

7.1. Überblick

Die vom Bundesverfassungsgericht entwickelten Grundsätze für den Schutz des Persönlichkeitsrechts bei der Erhebung und Verarbeitung personenbezogener Daten haben auch im Bereich der Rechtspflege einen Bedarf an der Schaffung neuer und an der Überarbeitung bestehender Rechtsvorschriften deutlich werden lassen. Die gründliche Analyse dieses Bedarfs und die Erarbeitung von Vorschlägen für dessen Umsetzung in ein verfassungsgemäßes Normenwerk im einzelnen ist ein langwieriger Prozeß, der die Datenschutzbeauftragten und die Justizverwaltungen wohl noch auf Jahre hinaus beschäftigen wird. Insgesamt gesehen kann jedenfalls ein in erfreulichem Maße gestiegenes Bewußtsein für einen solchen Handlungsbedarf in Teilbereichen der für die Justiz geltenden Rechtsnormen festgestellt werden. In jüngster Zeit hat sich auch die Arbeitsgruppe Datenschutz des Deutschen Richterbundes dieser Thematik angenommen.

Zu den Teilbereichen, in denen eindeutig ein Bedarf an der Schaffung gesetzlicher Regelungen besteht, gehören die „Anordnung über Mitteilungen in Zivilsachen (MiZi)" und die „Anordnung über Mitteilungen in Strafsachen (MiStra)", über die ich nachfolgend noch gesondert berichte. Neben diesen Problemkreisen wird insbesondere dem Bereich der Strafprozeßordnung künftig vermehrte Aufmerksamkeit zu widmen sein. In Ermittlungs- und Strafverfahren fallen regelmäßig eine Vielzahl personenbezogener Daten unterschiedlichster Art an, über den Beschuldigten, Anzeigeerstatter, Zeugen usw. Die Strafprozeßordnung regelt den Umgang der Justiz mit diesen Daten nach heutigem Datenschutzverständnis nur unvollkommen. Neuartige Fahndungsmethoden und Fahndungshilfsmittel zur Aufklärung von Straftaten bedürfen ebenso einer bereichsspezifischen Regelung wie manche der bisher nur in den „Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV)" geregelten Probleme. Ich erinnere insoweit nur an die in Nr. 185 und 185 a RiStBV geregelte Akteneinsicht, über die ich in meinen letzten beiden Tätigkeitsberichten nähere Ausführungen gemacht habe. Viele der in den vergangenen Jahren punktuell aufgegriffenen Fragen aus dem Bereich der Aufbewahrung und Weitergabe personenbezogener Daten durch die Staatsanwaltschaft stehen letztlich in einem Gesamtzusammenhang, der im Zuge einer Novellierung der Strafprozeßordnung einer einheitlichen, von den gleichen Leitgedanken getragenen Lösung zugeführt werden sollte. In diesem Zusammenhang werden auch Probleme des Verhältnisses der Staatsanwaltschaft zur Polizei aufzugreifen sein, die sich durch die rasch gewachsenen automatisierten Informationssysteme der Polizei und das dadurch entstandene faktische Informationsübergewicht der Polizei für die Stellung der Staatsanwaltschaft als „Herrin des Ermittlungsverfahrens" ergeben.

Es sei hier ferner auf die unter dem Stichwort „Verbesserung der Rechtsstellung des Verletzten im Strafverfahren" oder „Opferschutz im Strafverfahren" geführte Diskussion hingewiesen, bei der es bekanntlich u.a. auch um ein Anliegen des Persönlichkeitsschutzes geht, nämlich des Schutzes der Privatsphäre von als Zeugen vernommenen Tatopfern. Verschiedene Gesetzesinitiativen im parlamentarischen Raum und etwa die Befassung des Deutschen Juristentages 1984 mit dieser Thematik zeigen, welche Bedeutung der Lösung dieses Problems – meines Erachtens zu Recht – beigemessen wird. Einen nicht unwesentlichen Schwerpunkt der Diskussion bildet dabei die Frage, ob und gegebenenfalls wie eine Verbesserung des Opferschutzes durch Einschränkung der Öffentlichkeit von Strafverfahren herbeigeführt werden kann. Auch diese Fragestellung betrifft allerdings letztlich nur einen Ausschnitt aus einer umfassenderen Problematik, die sich als Spannungsfeld zwischen dem Grundsatz der Verfahrensöffentlichkeit einerseits und dem Schutz der Privatsphäre andererseits grundsätzlich in bezug auf alle Verfahrensbeteiligten und in allen Gerichtsverfahren stellt.

Meine nachfolgenden Ausführungen beschränken sich auf einige grundlegende Schwerpunkte im Bereich der Rechtspflege einschließlich des Strafvollzugs. Von den weiteren, hier nicht näher ausgeführten Themenkreisen, mit denen ich in den letzten zwölf Monaten befaßt war, seien hier nur stichwortartig genannt: Datenschutz im Notariat, automatisierte Datenverarbeitung im Gerichtsvollzieherbüro, Datenschutz im Grundbuchwesen und Fragen der Strafverfolgungsstatistik.

7.2. Mitteilungen in Zivilsachen

Aufgrund der bundeseinheitlichen Anordnung über Mitteilungen in Zivilsachen (MiZi) haben die Gerichte in Zivilverfahren in einer Vielzahl von Fällen Mitteilungen an andere Gerichte oder Behörden zu machen. Wie in meinem letzten Tätigkeitsbericht näher ausgeführt, halten die Datenschutzbeauftragten des Bundes und der Länder eine grundlegende Überprüfung dieser Anordnung durch die Justizverwaltungen in Bund und Ländern für erforderlich. Um nur einige wesentliche Kriterien einer solchen Überprüfung nochmals zu nennen: Es geht insbesondere darum, Mitteilungen, für die aus heutiger Sicht kein

hinreichendes sachliches Bedürfnis mehr besteht, entfallen zu lassen, den Umfang der einzelnen Mitteilungen ggf. auf das für den Empfänger notwendige Maß zu beschränken und für jene Mitteilungen, die bisher nicht auf einer gesetzlichen Grundlage beruhen, aber weiterhin für erforderlich gehalten werden, eine ausreichende gesetzliche Grundlage zu schaffen. Wegen weiterer Einzelheiten darf ich auf meine Ausführungen im 6. Tätigkeitsbericht unter Nr. 4.2.1 verweisen.

Die Justizverwaltungen haben eine Überprüfung dieser umfangreichen Materie zwischenzeitlich in Angriff genommen. Auch ein Arbeitskreis der Datenschutzbeauftragten des Bundes und der Länder hat sich intensiv mit den einzelnen Abschnitten der MiZi befaßt und das Ergebnis in Prüfungsbemerkungen niedergelegt. Danach läßt sich folgende vorläufige Bilanz ziehen: Die Mehrzahl der Mitteilungen scheint auch heute noch ihre sachliche Berechtigung zu haben; jedoch kann der Umfang vieler Mitteilungen reduziert werden. Zwei Fallgruppen mögen dies beispielhaft veranschaulichen:

- Enthält eine gerichtliche Entscheidung eine Personenstandsänderung oder eine sonstige in einem Personenstandsbuch einzutragende Tatsache, so ist es sicherlich sachgerecht, den die Personenstandsbücher führenden Standesbeamten von dieser Tatsache in Kenntnis zu setzen. Die Mitteilung an den Standesbeamten braucht jedoch nur jene Angaben zu umfassen, die der Standesbeamte zur Fortführung der Personenstandsbücher benötigt. Insoweit habe ich Zweifel, ob die in manchen Fällen vorgesehene Übersendung der vollständigen Entscheidung mit Gründen (vergl. MiZi Nr. VIII/1, XIII/7, XIII/16) erforderlich ist. Selbst die bei Ehescheidungsurteilen in der Regel vorgesehene Mitteilung nur der Entscheidungsformel (ohne Tatbestand und Gründe, vergl. MiZi Nr. VII/4) kann noch zu weitgehend sein, etwa wenn die Entscheidungsformel neben dem Ausspruch über die Scheidung auch Entscheidungen über Folgesachen wie z.B. die elterliche Sorge oder den Vorsorgungsausgleich enthält.

- Ändert sich durch eine gerichtliche Entscheidung der Name einer Person, die im Bundeszentralregister eingetragen ist, so kann das Register die ihm gesetzlich zugewiesene Funktion nur erfüllen, wenn es von dieser Namensänderung Kenntnis erlangt. Gegen die Unterrichtung des Bundeszentralregisters über die Namensänderung ist daher grundsätzlich nichts einzuwenden. Es ist jedoch nicht ersichtlich, daß der Registerbehörde zu diesem Zweck die vollständige Entscheidung mit Tatbestand und Gründen mitgeteilt werden müßte, wie es die MiZi derzeit noch vorsieht (vergl. MiZi Nr. VII/5, VIII/2, XIII/8, XIII/16, XIV/2).

Die vom Arbeitskreis der Datenschutzbeauftragten erarbeiteten umfangreichen Prüfungsbemerkungen, deren Abdruck den Rahmen dieses Tätigkeitsberichts sprengen würde, sollen den Justizverwaltungen für deren weitere Überlegungen zur Verfügung gestellt werden. Die Konferenz der Datenschutzbeauftragten hat am 13. September 1985 folgenden Beschluß gefaßt:

1. Die Datenschutzbeauftragten des Bundes und der Länder nehmen auf ihren Beschluß vom 6./7. Juni 1984 und die darin enthaltenen Empfehlungen für eine alsbaldige grundlegende Überprüfung der bundeseinheitlichen Anordnung über Mitteilungen in Zivilsachen (MiZi) Bezug. Vor diesem Hintergrund begrüßen sie die vom Bundesminister der Justiz im Zusammenwirken mit den Landesjustizverwaltungen eingeleitete umfassende Prüfung der MiZi.

2. Die Konferenz der Datenschutzbeauftragten hat parallel hierzu durch einen Arbeitskreis einzelne Abschnitte der MiZi unter datenschutzrechtlichen Gesichtspunkten prüfen lassen. Das Ergebnis dieser Prüfung ist in der Anlage zusammengestellt. Es ist nicht etwa in dem Sinne als umfassend anzusehen, daß alle denkbaren datenschutzrechtlichen Gesichtspunkte behandelt wären. Die Konferenz empfiehlt, die in der Zusammenstellung enthaltenen Bemerkungen bei den Beratungen der Justizverwaltungen und der Vorbereitung des Entwurfs einer gesetzlichen Regelung zu berücksichtigen. Die Datenschutzbeauftragten gehen davon aus, daß ihnen rechtzeitig Gelegenheit zur Stellungnahme gegeben wird, sobald ein Gesetzentwurf vorliegt.

3. In Anknüpfung an die in dem Beschluß vom 6./7. Juni 1984 gegebenen grundlegenden Empfehlungen für die Überprüfung der MiZi wird nochmals hervorgehoben, daß sie sich nicht nur auf die Erforderlichkeit und die Rechtsgrundlagen der Mitteilungen beziehen, sondern auch deren Umfang, Inhalt und Form einschließen sollte.

4. Soweit für einzelne Mitteilungen von den Justizverwaltungen als „mittelbare Rechtsgrundlagen" bezeichnete Rechtsgrundlagen bestehen, die sich auf die Aufgaben des Empfängers der Mitteilungen beziehen, so können diese ein Indiz für die Erforderlichkeit der Übermittlung sein, jedoch notwendige bereichsspezifische Rechtsgrundlagen für die Zulässigkeit der Übermittlung nicht ersetzen.

5. In Ergänzung der schon gegebenen Empfehlungen sollten auch folgende Prinzipien zum Tragen kommen:

   a) Die Übermittlungsvorgänge sollten transparenter gestaltet werden. Das Unbehagen vieler Bürger beim Umgang mit der öffentlichen Verwaltung rührt oftmals daher, daß diese über Kenntnisse verfügt, deren Herkunft den Betroffenen unbekannt ist. Wo es ohne unzumutbaren Aufwand möglich ist, sollte daher grundsätzlich vorgesehen werden, den Betroffenen von den Mitteilungen in geeigneter Weise zu unterrichten.

   b) Bei der Bestimmung der Empfängerbehörde sollte auf einen funktionalen Behördenbegriff abgestellt werden. Eine genaue Bezeichnung des Empfängers (z.B. Jugendamt, Straßenverkehrsamt) dient Anforderungen, die das Bundesverfassungsgericht an die präzise Bestimmung des Verwendungszwecks geknüpft hat.

   c) Der Eingriffscharakter von Mitteilungen tritt besonders bei solchen an die Finanzbehörde hervor. Die Notwendigkeit solcher nur im überwiegenden Allgemeininteresse zulässigen Eingriffe sollte unter Gesichtspunkten des in § 93 Abs. 1 Satz 3 der Abgabenordnung verankerten Subsidiaritätsprinzips geprüft werden, wonach andere Personen bzw. Stellen, als die Betroffenen selbst, erst dann zu einer

Auskunft (bzw. Mitteilung) heranzuziehen sind, wenn die Sachverhaltsaufklärung durch die Betroffenen nicht zum Ziele führt oder keinen Erfolg verspricht.

7.3. Mitteilungen in Strafsachen

Bereits seit meinem 3. Tätigkeitsbericht befasse ich mich regelmäßig mit den „Mitteilungen in Strafsachen". So habe ich auch an den entsprechenden Beschlüssen und Stellungnahmen der Datenschutzbeauftragten maßgebend mitgewirkt. Selbst der Beirat beim Landesbeauftragten für den Datenschutz hat sich dieses Themas in einer Reihe von Sitzungen intensiv angenommen. Kernpunkte der Diskussion waren die Notwendigkeit der Schaffung einer klaren Rechtsgrundlage und eine deutliche Verringerung der Mitteilungen auf das im Lichte neueren Verfassungsverständnisses erforderliche Maß.

Zum 1. April 1985 ist vom Bundesminister der Justiz und den Justizministern und -senatoren der Länder bundeseinheitlich eine Neufassung der Anordnung über Mitteilungen in Strafsachen (MiStra) in Kraft gesetzt worden (für Bayern siehe JMBl 1985 S. 42). Diese Neufassung der MiStra soll nach dem Verständnis der Justizminister nur für eine Übergangszeit gelten. Die nach wie vor bestehende Notwendigkeit einer hinreichend bestimmten gesetzlichen Grundlage erkennen die Justizminister ausdrücklich an. Die Neufassung der MiStra schränkt zwar einzelne bisher bestehende Mitteilungspflichten ein, im übrigen entspricht sie aber weitgehend der bisherigen Formulierung. Die Anregungen der Datenschutzbeauftragten sind leider nur zu einem Teil berücksichtigt worden. Die wesentlichen Kritikpunkte an der MiStra bestehen fort. Damit bleibt die Schaffung eines entsprechenden Gesetzes dringlich.

Die Vorbereitung für eine solche gesetzliche Regelung für Mitteilungen aus Strafverfahren ist nach Mitteilung des Staatsministeriums der Justiz eingeleitet. Das Justizministerium hält eine bundesgesetzliche Regelung für erforderlich. Offensichtlich bestehen derzeit noch Meinungsverschiedenheiten über deren Konzeption. Diese berühren teilweise verfassungsrechtliche Fragen, insbesondere nach der Gesetzgebungskompetenz des Bundes. Infolge dieser Frage wird erörtert, inwieweit der Bundesgesetzgeber nur ein sogenanntes Rahmengesetz erlassen, das durch entspechende Länderregelungen zu ergänzen wäre, oder ein Bundesmitteilungsgesetz schaffen soll. In letzterem würde der Bund die gesetzlichen Grundlagen für die Mitteilungen in Strafsachen vollständig und abschließend regeln. Aus der Sicht des Datenschutzes würde ich der letztgenannten Konzeption eindeutig den Vorzug geben. Meines Erachtens kann nur durch eine bundeseinheitliche Regelung sichergestellt werden, daß die Mitteilungen in eindeutiger und verfassungskonformer Weise bundesweit einheitlich vollzogen werden. Ich begrüße es, daß das Bayerische Staatsministerium der Justiz das Modell eines Bundesmitteilungsgesetzes strikt befürwortet.

Ein solches Bundesmitteilungsgesetz, das die Mitteilungstatbestände und die Mitteilungspflichten abschließend regelt, müßte meines Erachtens insbesondere folgenden datenschutzrechtlichen Belangen Rechnung tragen:

- Die Beachtung des Grundsatzes der Zweckbindung sollte durch eine ausdrückliche Bestimmung sichergestellt werden, wonach die Empfängerbehörden die mitgeteilten Daten nur für den Zweck verwenden dürfen, zu dessen Erfüllung sie zulässigerweise übermittelt worden sind.
- Der im Datenschutzrecht geltende, aus dem Prinzip der Verhältnismäßigkeit abgeleitete Grundsatz der Erforderlichkeit gebietet, die Mitteilungen und ihren Inhalt auf das im Einzelfall erforderliche Mindestmaß zu beschränken. Es sollte daher sichergestellt werden, daß Mitteilungen tatsächlich nur dann gemacht werden, wenn sie für die empfangende Stelle entscheidungserheblich sind. Auch müßte wohl das derzeit bestehende Regel-Ausnahmeverhältnis zum Inhalt der Mitteilungen umgekehrt werden mit der Folge, daß grundsätzlich nur der Anklagesatz oder die Urteilsformel mitgeteilt wird. Bei der Festlegung des Zeitpunkts der jeweiligen ersten Mitteilung ist zu berücksichtigen, das sich strafrechtlich relevante Sachverhalte erst nach rechtskräftigem Abschluß eines Strafverfahrens abschließend beurteilen lassen. Vorzeitige Mitteilungen sollten daher die Ausnahme bilden.
- Die Anordnung von Mitteilungen ist jedenfalls dann dem Richter oder dem Staatsanwalt vorzubehalten, wenn der sachgerechte Vollzug eine Abwägung im Einzelfall voraussetzt. Nur wenn es gelingt, Anlaß, Inhalt und Zeitpunkt der Mitteilungen abschließend und eindeutig festzulegen, können diese auch vom Beamten der Geschäftsstelle angeordnet werden.
- Die Zeitdauer der Aufbewahrung und Verwertung der entsprechenden Mitteilungen sollte vergleichbar den im Bundeszentralregistergesetz enthaltenen Verwertungsgrundsätzen geregelt werden.
- Gerade im Hinblick auf das durch das informationelle Selbstbestimmungsrecht dem Betroffenen eingeräumte Recht, zu wissen, wer, was, wann über ihn weiß, sollte der Betroffene grundsätzlich über die seine Person betreffenden Mitteilungen unterrichtet werden.

Ich beabsichtige, mich auch künftig mit Fragen der „Mitteilungen in Strafsachen" zu befassen.

7.4. Schuldnerverzeichnis

Über Probleme des beim Amtsgericht geführten Schuldnerverzeichnisses habe ich schon mehrfach, zuletzt ausführlich in meinem 6. Tätigkeitsbericht, berichtet. In das Schuldnerverzeichnis werden Personen eingetragen, die die eidesstattliche Versicherung über ihr Vermögen abgegeben haben oder gegen die wegen Nichtabgabe der eidesstattlichen Versicherung Haft angeordnet ist. Das Schuldnerverzeichnis dient dem Schutz des soliden Geschäftsverkehrs vor unzuverlässigen Schuldnern. Über das Bestehen oder Nichtbestehen einer bestimmten Eintragung ist jedermann auf Antrag Auskunft zu erteilen. Dadurch soll u.a. ein Anreiz für den Schuldner entstehen, seine Schuld zu bezahlen; denn durch den Nachweis der Befriedigung des Gläubigers kann der Schuldner die vorzeitige Löschung der Eintragung erreichen. In jedem Fall hat der Schuldner einen Anspruch auf Löschung nach Ablauf von drei Jahren seit dem Schluß des Eintragungsjahres.

Wenn auch jedermann auf Verlangen Auskunft darüber zu geben ist, ob eine bestimmte Person im Schuldnerverzeich-

nis eingetragen ist, so hat das Schuldnerverzeichnis doch nach den gesetzlichen Vorschriften nur eine eingeschränkte Publizität. So ist die Veröffentlichung des Verzeichnisses in Druckerzeugnissen, die jedermann zugänglich sind, nicht gestattet. Abschriften aus dem Verzeichnis dürfen nur erteilt und entnommen werden, wenn die Einhaltung der Löschungsfristen gesichert erscheint. Bereits in meinem 3. Tätigkeitsbericht hatte ich die derzeitige, auf einer Verwaltungsvorschrift des Bundesministers der Justiz beruhende Praxis der Erteilung von Abschriften als änderungsbedürftig bezeichnet, da die Einhaltung der Löschungsfristen nicht bei allen Empfängern gewährleistet sein dürfte. Meine nachfolgenden Ausführungen sollen diese immer noch ungelöste Problematik etwas anschaulicher werden lassen.

Die Industrie- und Handelskammer für München und Oberbayern (IHK) erhält jeweils zum 1. und 15. eines jeden Monats von den bayerischen Amtsgerichten die jeweiligen im zurückliegenden 14-Tage-Zeitraum angefallenen Neueintragungen und vorzeitigen Löschungen im Schuldnerverzeichnis mitgeteilt. Die IHK gibt ihrerseits im 14-tägigen Turnus vertrauliche „Schuldnerlisten" heraus. Diese kann jeder beziehen, der einer berufsständischen Einrichtung (z.B. IHK, Handwerkskammer, Rechtsanwaltskammer) zugehörig ist, ein berechtigtes Interesse am Bezug glaubhaft macht und sich den Bezugsbedingungen unterwirft. In den Bezugsbedingungen ist auf das Verbot der Weitergabe, Vervielfältigung, Veröffentlichung usw. sowie auf die Löschungspflichten hingewiesen. Die Anzahl der Bezieher der IHK-Schuldnerliste soll sich in einer Größenordnung von rund 2.000 bewegen. Die IHK-Schuldnerliste für ganz Bayern enthält, bezogen auf einen Zeitraum von 14 Tagen, jeweils mehrere tausend Neueintragungen und mehrere hundert vorzeitige Einzellöschungen. Ein regelmäßiger Bezieher dieser Liste, der die Listen aufbewahrt, muß also, um der Löschungsverpflichtung nachzukommen, alle 14 Tage anhand der Liste über die vorzeitigen Löschungen mehrere hundert Eintragungen in den früheren Listen heraussuchen und unkenntlich machen.

Diese Größenordnungen machen m.E. deutlich, welche praktische Bedeutung das aufgeworfene Problem hat. Die Gefahr, daß überholte Eintragungen gegen den Willen des Gesetzgebers nicht immer gelöscht werden, liegt auf der Hand. Die Verwendung solcher nicht berichtigter Daten kann aber für die Betroffenen erhebliche nachteilige Auswirkungen wie Rufschädigung und Bewertung als kreditunwürdig haben. Wie konkret die hier aufgezeigten Risiken tatsächlich sind, zeigt besonders drastisch ein Vorfall aus Baden-Württemberg, über den die Presse kürzlich berichtete: Danach wurden in Stuttgart Schuldnerlisten mit den Namen und Adressen von rund 10.000 Schuldnern aus den Jahren 1977 bis 1980 auf dem Sperrmüll gefunden. Die Liste soll von einem der rund 2.000 Mitglieder eines Gläubigerschutzverbandes stammen. Offenbar waren weder das Verbot der pauschalen Weitergabe solcher Listen noch die Löschungsvorschriften der Zivilprozeßordnung beachtet worden.

Ferner habe ich festgestellt, daß in einer mir vorliegenden IHK-Schuldnerliste rund ein Drittel aller Eintragungen kein über Namen und Anschrift hinausgehendes Identifikationsmerkmal (Geburtsdatum und ggf. Beruf) aufweist. Über die sich hierdurch ergebende Gefahr von Personenverwechselungen, wie sie in der Praxis tatsächlich vorgekommen sind, habe ich im letzten Tätigkeitsbericht berichtet. Das Fehlen zusätzlicher Identifikationsmerkmale kann allerdings weder der IHK noch dem Amtsgericht angelastet werden, wenn das Amtsgericht – wie es häufig bei Eintragungen wegen Haftanordnung der Fall ist – das Geburtsdatum und den Beruf des Schuldners nicht kennt und deshalb auch nicht eintragen und nicht der IHK übermitteln kann. Tatsächlich betrafen die von mir gefundenen Eintragungen ohne zusätzliche Identifikationsmerkmale fast ausschließlich den Eintragungsgrund der Haftanordnung. Die Größenordnung von rund ein Drittel aller Fälle ohne Angabe des Geburtsdatums zeigt jedoch, daß die Gefahr von Personenverwechslungen nach wie vor im Auge behalten werden muß und daß über Lösungen dieses Problems nachzudenken sein wird.

Dem Vernehmen nach werden die Vorarbeiten an einer Neugestaltung der Vorschriften über das Schuldnerverzeichnis nunmehr in verstärktem Maße vorangetrieben. Ich habe in diesem Zusammenhang noch folgende Anregungen für eine Neuregelung gegeben:

- Für die Löschung nach Ablauf der 3-Jahres-Frist setzt das Gesetz seinem Wortlaut nach einen Antrag des Schuldners voraus. Dieses Antragserfordernis sollte entfallen und die Eintragung nach Fristablauf von Amts wegen gelöscht werden. Ein erhöhter Verwaltungsaufwand wäre insoweit wohl nicht zu befürchten, da die nach der Aktenordnung ohnehin nach fünf Jahren von Amts wegen vorzunehmende Löschung insoweit nur zeitlich vorverlagert würde.

- Der Anspruch auf Löschung nach Fristablauf besteht nach derzeitiger Rechtslage nicht schon nach Ablauf von 3 Jahren seit dem Tage der Abgabe der eidesstattlichen Versicherung oder der Anordnung der Haft; vielmehr hat das Gesetz aus Gründen der Praktikabilität den Fristablauf jeweils einheitlich auf den Schluß des Kalenderjahres gelegt. Verschiedene Rechtsfolgen der eidesstattlichen Versicherung oder der Haftanordnung sind jedoch an eine 3-jährige Schutzfrist geknüpft, die bereits 3 Jahre nach dem Tag der Abgabe der eidesstattlichen Versicherung oder der Anordnung der Haft endet. Es wäre daher wohl sachgerecht, die eingetragenen Daten nach Ablauf dieser 3-jährigen Schutzfrist bis zur – nur aus Praktikabilitätsgründen auf das Ende des Kalenderjahres hinausgeschobenen – tatsächlichen Löschung nicht weiter zu verwenden, d.h. insbesondere keine Auskunft mehr über die Eintragung zu geben.

- Durch die Eingabe eines Bürgers bin ich ferner auf die Problematik derjenigen Fälle gestoßen, in denen vor Fristablauf der die Eintragung bewirkende Tatbestand nachträglich weggefallen ist. Im konkreten Fall des Petenten hatte das Beschwerdegericht festgestellt, daß das Vollstreckungsgericht die Voraussetzungen für den Erlaß einer Haftanordnung zu Unrecht angenommen hatte. Die Haftanordnung wurde deshalb aufgehoben. Damit war auch die Eintragung im Schuldnerverzeichnis materiell unrichtig geworden. Ob in einem solchen Fall die Löschung der Eintragung – wie ich meine – von Amts wegen zu erfolgen hat, oder einen entsprechenden Löschungsantrag des Schuldners voraussetzt, wird in der juristischen Literatur nicht einheitlich beantwortet. Im konkreten Fall jedenfalls stand der Petent, der von einem

etwaigen Antragserfordernis keine Kenntnis hatte, noch Monate nach der Haftaufhebung – materiell zu Unrecht – im Schuldnerverzeichnis. Es sollte deshalb erwogen werden, für diese Fallkonstellation eine Löschungspflicht von Amts wegen ausdrücklich gesetzlich vorzusehen.

7.5. Weitergabe gerichtlicher Entscheidungen

In meinem 5. Tätigkeitsbericht hatte ich auf den Grundsatz hingewiesen, daß in gerichtlichen Entscheidungen, die an am Gerichtsverfahren nicht beteiligte Stellen übermittelt werden, die Namen und sonstige zur Identifizierung geeignete Merkmale unkenntlich zu machen sind. Etwas anderes kann grundsätzlich nur dann gelten, wenn die Mitteilung der Entscheidung zur Information über die von der Entscheidung betroffene konkrete Person dienen soll und die empfangende Stelle diese Information aufgrund verfassungsgemäßer Rechtsvorschriften erhalten darf. Diese Ausnahme liegt bei einem Austausch von Gerichtsentscheidungen zwischen Behörden zum Zwecke der bloßen Information über die auf einem bestimmten Gebiet ergangene Rechtsprechung nicht vor.

Ein Beispiel für einen solchen Austausch gerichtlicher Entscheidungen ist die unter den Generalstaatsanwälten stattfindende gegenseitige Information über bedeutsame Entscheidungen der Ehrengerichtshöfe für Anwaltssachen. Da es hierbei um die Unterrichtung über die Grundsätze der obergerichtlichen Rechtsprechung auf dem Gebiet der Ehrengerichtsbarkeit für Rechtsanwälte geht und nicht etwa um die Information über einzelne betroffene Rechtsanwälte, habe ich angeregt, künftig bei der Übersendung von Entscheidungen der genannten Art Namen und Anschrift des Betroffenen unkenntlich zu machen. Das Bayerische Staatsministerium der Justiz hat mir mitgeteilt, daß solche Entscheidungen in seinem Geschäftsbereich künftig nur noch in anonymisierter Form versandt werden; entsprechende Anordnungen sind übrigens auch in anderen Bundesländern getroffen worden.

7.6. Strafvollzug

Auch im Bereich des Strafvollzugs besteht die Notwendigkeit, die derzeit für den Strafvollzug geltenden Regelungen daraufhin zu überprüfen, ob sie dem Gesichtspunkt des Persönlichkeitsschutzes unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts hinreichend Rechnung tragen. Dabei geht es sowohl um die Frage nach ausreichenden gesetzlichen Rechtsgrundlagen für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung, als auch um die verfassungsgemäße inhaltliche Ausgestaltung solcher Rechtsgrundlagen. Die Justizverwaltungen des Bundes und der Länder wollen sich dieser Thematik annehmen und haben den Bundesminister der Justiz um eine entsprechende Überprüfung und gegebenenfalls um die Vorlage von Vorschlägen für eine Neuregelung gebeten. Ich begrüße diese Initiative ausdrücklich und werde zu gegebener Zeit gemeinsam mit den Datenschutzbeauftragten der anderen Länder und des Bundes zu einer datenschutzgerechten Lösung beizutragen versuchen. Zunächst bleiben die diesbezüglichen Vorschläge des Bundesministers der Justiz abzuwarten.

Im Berichtszeitraum war ich mit verschiedenen allgemeinen Fragen und generellen Verwaltungsregelungen im Strafvollzug befaßt. So war ich z.B. an den Überlegungen der Justizverwaltungen zur Neugestaltung der Vordrucke beteiligt, mit denen Staatsanwaltschaften/Gerichte, das Landeskriminalamt und, soweit zutreffend, die Ausländerbehörde oder das Jugendamt von der Aufnahme oder Entlassung eines Gefangenen unterrichtet werden. Ein weiteres Thema, zu dem ich vom Bayerischen Staatsministerium der Justiz um Stellungnahme gebeten worden war, betraf die Datenübermittlung von der Justizvollzugsanstalt an die Meldebehörde zum Zwecke der melderechtlichen Erfassung von Gefangenen. Hier konnte ich einige Anregungen zur Beschränkung des Umfangs der zu übermittelnden Daten geben; diese Anregungen wurden aufgegriffen und verwirklicht.

Ferner hat mich das Bayerische Staatsministerium der Justiz auf meine Bitte hin von der Praxis unterrichtet, inwieweit die Justizvollzugsanstalten in Bayern bei Polizeidienststellen und anderen Behörden Auskünfte über Bezugspersonen erholen, bei denen Gefangene den Urlaub verbringen wollen. Es geht hierbei um folgendes: Die Justizvollzugsanstalten haben bei der Entscheidung über die Gewährung von Urlaub aus der Haft (§ 13 Strafvollzugsgesetz – StVollzG –) auch darauf zu achten, daß keine Mißbrauchsgefahr besteht und daß durch den Urlaub die Wiedereingliederung des Gefangenen gefördert oder jedenfalls nicht behindert wird. Diese Aufgabe wird u.a. durch Nr. 5 Abs. 1 der bundeseinheitlichen Verwaltungsvorschriften zu § 13 StVollzG konkretisiert. Danach darf der Gefangene in der Regel nicht in eine soziale Umgebung oder zu Personen beurlaubt werden, von denen aufgrund tatsächlicher Anhaltpunkte zu befürchten ist, daß sie seiner Eingliederung entgegenwirken. Um dies prüfen zu können, erholen die Justizvollzugsanstalten vielfach entsprechende Informationen von Stellen außerhalb des Vollzuges (z.B. Polizei, Gemeinde, Jugendamt, Bewährungshilfe, sonstige Betreuungsstelle). Die Verfahrensweise im einzelnen ist mit Rücksicht auf die unterschiedlichen Verhältnisse in den verschiedenen Anstalten nicht einheitlich und hängt gegebenenfalls auch von den jeweiligen Umständen des Einzelfalles ab. Die Thematik ist zur Zeit Gegenstand eines Erfahrungsaustausches unter den Landesjustizverwaltungen.

Bei den Eingaben von Gefangenen stand wiederum das Anliegen im Vordergrund, daß außenstehende Dritte möglichst nicht Kenntnis von der Inhaftierung erhalten. Ich habe über diese Problematik in meinem 6. Tätigkeitsbericht unter verschiedenen Gesichtspunkten ausführlich berichtet. Ergänzend dazu möchte ich hier auf die Frage eingehen, inwieweit Justizvollzugsanstalten an private Personen oder Stellen Auskünfte über Gefangene geben dürfen. Derartige Auskunftsersuchen werden beispielsweise von Personen gestellt, die Rechtsansprüche gegen einen Gefangenen geltend machen und deshalb – etwa zum Zwecke der Zustellung eines Mahnbescheides – wissen wollen, ob sich der Schuldner in der Justizvollzugsanstalt aufhält. Stimmt der Gefangene einer Auskunftserteilung nicht zu, so hat die Justizvollzugsanstalt nach Nr. 5 Abs. 3 Satz 3 Vollzugsgeschäftsordnung eine Abwägung der widerstreitenden Interessen – des Gefangenen einerseits, der auskunftsersuchenden Person andererseits – vorzunehmen (vergleiche Art. 18 Abs. 1 BayDSG). Das Oberlandesgericht Celle hat hierzu kürzlich folgende Auffassung vertreten (Beschluß

vom 21.9.1984, NStZ 1984, 44): Grundsätzlich könne dem Gläubiger, der ein berechtigtes Interesse (z.B. einen Zahlungsanspruch) an der Bekanntgabe des Aufenthaltsortes darlegt, auch ohne Einverständnis des Gefangenen die gewünschte Auskunft erteilt werden. Es dürfe jedoch nur die Information mitgeteilt werden, die zur Verfolgung dieses Interesses notwendig ist, also in der Regel nur der Aufenthalt des Gefangenen in der Anstalt, nicht aber der Zeitpunkt der Haftentlassung. Der Anfragende dürfe jedoch von einer in naher Zukunft bevorstehenden Haftentlassung unterrichtet werden, da sonst Maßnahmen, die der Anfragende im Vertrauen auf die Richtigkeit der Auskunft ergreift, ins Leere gehen könnten.

8. Städte und Gemeinden

8.1. Nutzung von Daten Steuerpflichtiger für andere Zwecke der Gemeinde?

Im Zuge von Datenschutzprüfungen habe ich festgestellt, daß in Gemeinden Namen, Anschriften und Grundstücksbezeichnungen aus Unterlagen des gemeindlichen Steueramts auch bei anderen Dienststellen der Gemeinde, etwa zum Zwecke der Festsetzung von Gebühren und Abgaben nach dem Kommunalabgabengesetz (KAG), Verwendung finden. Da sich hier die Frage der Reichweite des Steuergeheimnisses stellt, das nach dem KAG auch für kommunale Steuern gilt, habe ich das Bayerische Staatsministerium der Finanzen und das Bayerische Staatsministerium des Innern um Stellungnahme gebeten. Das Staatsministerium der Finanzen hat sich mehrfach auf den Standpunkt gestellt, die Verwendung von Daten aus einer gemeindlichen Grundsteuerdatei für Zwecke außerhalb des Bereichs der Abgabenordnung sei nicht zulässig. Der „Bereich der Abgabenerhebung" in diesem Sinne sei nur dann gegeben, wenn die Vorschriften der Abgabenordnung über das Steuergeheimnis unmittelbar oder entsprechend gelten (z.B. bei Realsteuern, soweit ihre Verwaltung den Gemeinden übertragen worden ist, nach § 1 Abs. 2 Nr. 1 AO; bei kommunalen Steuern und Fremdenverkehrsbeiträgen nach Art. 13 Abs. 1 Buchst. c KAG). Die Unzulässigkeit einer Weitergabe von Namen, Anschrift und Objekt eines Steuerpflichtigen vom gemeindlichen Steueramt an andere Dienststellen der Gemeinde stellt u.a. auch weite Teile der in Bayern gebräuchlichen Grundabgabeverfahren von Städten und Gemeinden in Frage (z.B. bei gemeinsamer Veranlagung von Grundsteuer, Müllabfuhr und Straßenreinigungsgebühren). Auch die Erstellung von „Objektlisten" aus den gemeindlichen Steuerunterlagen, die den mit der Festsetzung von KAG-Abgaben befaßten gemeindlichen Dienststellen als Arbeitsunterlage dient, wäre danach nicht zulässig.

Da eine Vermeidung der Nutzung der genannten Angaben aus den gemeindlichen Steuerunterlagen zu einem erheblichen Verwaltungsaufwand führen würde, nämlich zur eigenen Erhebung der mit der Festsetzung von KAG-Abgaben befaßten kommunalen Stellen, habe ich das Bayerische Staatsministerium des Innern inzwischen gebeten, Möglichkeiten zur Änderung des KAG zu überprüfen. Ungelöst bliebe hierbei allerdings nach wie vor die Frage der Weitergabe von Namen, Anschrift und Objekt des Steuerpflichtigen zum Zwecke der Festsetzung von Erschließungsbeiträgen nach dem Bundesbaugesetz an die dafür zuständigen Stellen. Ich halte es darüber hinaus nicht für ausgeschlossen, daß sich die Frage der Nutzbarkeit der vorgenannten Daten aus kommunalen Steuerunterlagen auch noch in anderem Zusammenhang stellt.

Im Interesse der Rechtssicherheit sollte hierzu möglichst bald eine befriedigende Lösung gefunden werden.

8.2. Das Personalamt einer Stadt und die „Freiwilligen Wahlhelfer"

Durch eine Eingabe wurde ich auf den folgenden Sachverhalt aufmerksam: Im Zuge von Wahlvorbereitungen hatte der Leiter eines städtischen Amtes eine Liste aller in der Abteilung tätigen Personen unter Angabe des Vor- und Zunamens, des Lebensalters, der Anschrift und der Gründe für eine evtl. Nichtbereiterklärung zur Übernahme eines Ehrenamtes im Rahmen der Wahl erstellt. Die vollständige Liste wurde vor der Zuleitung an das Wahlamt dem Personalreferenten vorgelegt. Ich habe zu diesem Sachverhalt folgendermaßen Stellung genommen:

Gemeindebürger sind nach Art. 19 BayGO zur Übernahme von Ehrenämtern verpflichtet und können diese nur aus wichtigen Gründen ablehnen. Ob der von einem Verpflichteten genannte Ablehnungsgrund ein wichtiger im Sinne des Art. 19 Abs. 2 BayGO ist, entscheidet nach Art. 19 Abs. 3 BayGO der Gemeinderat. Nach Auskunft der betreffenden Stadt sollte dort allerdings auf der Verpflichtung nach Art. 19 BayGO nicht bestanden werden. Die Bediensteten sollten nur auf freiwilliger Basis zu Wahlhelferdiensten herangezogen werden.

Eine Erhebung von Daten „freiwilliger" Wahlhelfer durch den Amtsleiter muß meines Erachtens ausscheiden. Er könnte jedoch eine Liste in Umlauf geben, die nach Ausfüllung direkt an das Wahlamt weitergeleitet wird. Eine Begründung, warum der Bedienstete keinen Wahldienst leisten kann oder will, sollte direkt durch das Wahlamt – ohne Beteiligung des Amtsleiters bzw. des Personalamtes – eingeholt werden, wenn die Zahl der freiwilligen Wahlhelfer nicht ausreicht. Einen Rücklauf der Liste über den Amtsleiter bzw. das Personalamt halte ich aus Gründen des Datenschutzes für bedenklich, da die ensprechenden Angaben nur für Wahlzwecke erhoben und verwendet werden dürfen.

Denkbar wäre auch, daß vom Personalreferat potentielle freiwillige Wahlhelfer dem Wahlamt benannt werden. Dabei dürfte allerdings die Übermittlung der Daten aller Bediensteten nicht erforderlich sein. So sollte auf die Übermittlung der Daten von Bediensteten, die nicht für die Ausübung von solchen Ämtern in Betracht kommen (z.B. längere Krankheit) verzichtet werden. Auf eine Angabe der Gründe, die gegen eine Benennung sprechen könnten, ist dabei meines Erachtens ebenfalls zu verzichten. Auch in einem solchen Falle wäre ein Rücklauf einer Liste über das Personalamt zu dessen rechtmäßiger Erfüllung der durch Rechtsnorm zugewiesenen Aufgaben meines Erachtens nicht erforderlich.

Die eigentliche Inanspruchnahme der Wahlhelfer, die im öffentlichen Dienst beschäftigt sind, sollte grundsätzlich im Wahlamt, also außerhalb der Personalverwaltung organisiert werden.

8.3. Darf ein Erschließungs-Beitragspflichtiger von der Gemeinde erfahren, wieviel seine Nachbarn für Grundstücksverkäufe erhalten haben?

Ein Gemeindebürger, der erschließungsbeitragspflichtig war im Sinne des § 134 Abs. 1 BBauG, hatte die Gemeinde um detaillierte Auskunft gebeten, wieviel seine Nachbarn für Grundstücksverkäufe, für Abbrucharbeiten und für Wiederaufrichtungsarbeit im einzelnen erhalten hätten.

Das von mir eingeschaltete Bayerische Staatsministerium des Innern hat in seiner Stellungnahme – der ich mich anschließe – folgende Ausführungen zu der über den einzelnen Fall hinaus interessanten Frage der Zulässigkeit der Offenbarung solcher Daten gemacht: Für den Verfahrensbereich „Stellung der Beteiligten im Verfahren" hat Art. 13 Abs. 1 Nr. 3 Buchst. b des Kommunalabgabengesetzes (KAG) die einschlägigen Vorschriften der Abgabenordnung (§§ 85 und 93) für anwendbar erklärt. Wenn dabei in der Abgabenordnung eine dem Art. 29 des Bayerischen Verwaltungsverfahrensgesetzes entsprechende Vorschrift fehlt, beruht dies auf der Entscheidung des Gesetzgebers, den Beteiligten in Abgabensachen kein allgemeines Recht auf Akteneinsicht einzuräumen, sondern die Form der Gewährung rechtlichen Gehörs im Rahmen des § 91 AO in das Ermessen der Behörde zu stellen. Eine Anwendung des Art. 29 BayVwVfG dürfte damit in Erschließungsbeitragssachen ausscheiden.

In welcher Form und in welchem Umfang den Beitragspflichtigen Auskunft über die entstandenen Grunderwerbs- und Freilegungskosten zu gewähren ist, ist damit von der Gemeinde unter einzelfallbezogener Abwägung der widerstreitenden Interessen der Betroffenen zu entscheiden. Für diese Abwägung könnten die Überlegungen herangezogen werden, die die Obersten Aufsichtsbehörden für den Datenschutz zu vergleichbaren Fällen von Rechnungslegung im Privatbereich (Mitteilung von Hausmeistereinkünften an Mieter zur Überprüfung der Nebenkostenabrechnung) entwickelt haben. Danach sei ein Aufschlüsseln der Gesamt-Hausmeisterkosten in Lohnkosten, Geldwerte, Leistung, Sozialabgaben etc. im Rahmen der Gesamtabrechnung nicht erforderlich. Die der Berechnung zugrundeliegenden Belege seien vom Eigentümer zur Einsichtnahme und Prüfung bereitzuhalten, so daß dem Mieter, wenn er Zweifel an der Richtigkeit der Abrechnung hat, eine Kontrolle möglich sei. Da in einem solchen Falle Informationsbedürfnisse der Mieter mit dem Interesse des Hausmeisters am Schutz persönlicher Belange kollidieren können, muß der Hausmeister damit rechnen, daß sein Einkommen den Mietern offenbart wird. Doch sollten seine schutzwürdigen Belange nicht völlig außer acht gelassen werden. Deshalb sollte darauf abgestellt werden, ob Anhaltspunkte vorliegen, die tatsächlich auf eine fehlerhafte Abrechnung schließen lassen. Die Überprüfungsmöglichkeit sollte nur auf ein begründetes Verlangen hin gewährt und dabei ein Verfahren gewählt werden, das für die Betroffenen das schonendste Mittel darstellt (z.B. Aufschlüsselung nach einzelnen Gebäuden bei größeren Gebäudekomplexen).

Bei der Entscheidung ist mit zu berücksichtigen, daß die Aufstellung über die Grunderwerbs- und Freilegungskosten jedenfalls dem Verwaltungsgericht auf Verlangen vorzulegen ist; in die Gerichtsakten können die Beteiligten Einsicht nehmen (§ 100 VWGO).

8.4. Antrag auf Erteilung eines Führungszeugnisses mit falschen Angaben

Ein Bürger, der sich an mich gewandt hatte, teilte mit, er habe von der Dienststelle des Bundeszentralregisters eine Mitteilung erhalten, daß sich die Erteilung eines beantragten Führungszeugnisses zur Vorlage bei der Gemeinde – zum Zwecke einer Bewerbung – verzögere. Ich habe daraufhin festgestellt, daß die Gemeinde selbst über den Petenten ein Führungszeugnis beantragt hatte. Sie teilte mir als Grund hierfür mit, daß der Inhalt des Führungszeugnisses dafür hätte verwendet werden sollen, über eine evtl. Vorstrafe des Petenten den Gemeinderat zu unterrichten damit er gegebenenfalls von der Absicht, Strafantrag gegen den Petenten in einer – privatrechtlichen – Grundstücksangelegenheit zu stellen, Abstand nehmen könnte. Nun können zwar nach § 29 des Bundeszentralregistergesetzes Behörden über eine bestimmte Person ein Führungszeugnis erhalten, wenn sie es zur Erledigung hoheitlicher Aufgaben benötigen und eine Aufforderung an den Betroffenen, ein Führungszeugnis vorzulegen, nicht sachgemäß ist oder erfolglos bleibt. Die Gemeinde hatte aber zu diesem Mittel in Zusammenhang mit einer zivilrechtlichen Auseinandersetzungen über Maßnahmen an einem gemeindlichen Grundstück gegriffen, nicht jedoch zur Erledigung hoheitlicher Aufgaben. Die Gemeinde hatte den Antrag auf Erteilung des Führungszeugnisses auch nicht mit der privatrechtlichen Auseinandersetzung begründet, sondern „Bewerbung" als Verwendungszweck angegeben.

Die Gemeinde hatte damit versucht, in einem gesetzlich nicht vorgesehenen Fall Informationen aus dem Bundeszentralregister zu erlangen und zu diesem Zweck eine falsche Angabe zum Betroffenen an das Bundeszentralregister übermittelt.

Ich habe dies gegenüber der Gemeinde festgestellt und gemäß Art. 29 BayDSG hiervon die zuständige Aufsichtsbehörde und den Beirat verständigt.

8.5. Nach dem Urlaub kommt die Polizei

In einer Eingabe wurde Beschwerde darüber geführt, daß der ehrenamtliche Vorsitzende des Verkehrsvereins, der gleichzeitig Polizeibeamter sei, vor Beherbergungsstätten auswärtige Kfz-Kennzeichen notiert habe. Im Anschluß daran seien offenbar die Halter festgestellt und die in ihre Heimatorte zurückgekehrten Gäste durch die jeweilige Polizeidienststelle wegen der Kurbeiträge befragt worden.

Die Eingabe veranlaßte mich zu prüfen, ob diese Art der Datenerhebung u.a. dem Grundsatz der Verhältnismäßigkeit der Mittel entsprach. Ich bat die Gemeinde zu klären, ob eine den Gast weniger belastende Vorgehensweise bei der Erhebung personenbezogener Daten durchführbar wäre. Denkbar wäre z.B. daß ein gemeindlicher Kontrolleur direkt beim Leiter der Beherbergungsstätte um Vorlage der Beherbergungsmeldescheine gemäß Art. 27 Abs. 4 MeldeG bäte. Soweit von den Besitzern der PkW, die vor dem Betrieb abgestellt sind, solche Meldescheine fehlen, kann der Sachverhalt an Ort und Stelle mit dem Leiter der Beherbergungsstätte, der für den Kurbeitrag haftet, aufgeklärt werden. Dieses könnte als geeignetes gleichwohl

aber gelinderes Mittel im Verhältnis zur Einvernahme der Gäste durch die Polizei an ihrem Wohnort angesehen werden. Der Gemeinderat beschloß daraufhin, daß das Aufsuchen der Gäste in ihren Heimatorten durch die Polizei künftig vermieden werden sollte. Ein Gemeindebediensteter werde künftig unmittelbar bei den Beherbergungsbetrieben kontrollieren.

8.6. Fehlsubventionen im Wohnungswesen:

Darf nach Einkommensarten gefragt werden, die in die Berechnung für die Ausgleichsabgabe nicht einbezogen werden dürfen?

In einer Eingabe wurde kritisiert, eine Stadt frage im Vollzug des Gesetzes zum Abbau der Fehlsubventionierung des Wohnungswesens in der „Einkommenserklärung" nach verschiedenen Rentenarten (z.B. KB-Rente), die nach dem Gesetz nicht zum anrechenbaren Einkommen gehören. Ein entsprechender Hinweis im Sinne von Art. 16 Abs. 2 BayDSG auf Pflicht- bzw. freiwillige Antworten fehlte.

Die Stadt wollte Angaben über solche nicht anrechenbaren Einkunftsarten erheben, um einen Überblick über die Einkommensverhältnisse der Betroffenen zu gewinnen. In einem Gespräch mit der Stadt wurde Einigkeit darüber erzielt, daß es sich bei den Angaben der Kriegsschadensrente und der Hinterbliebenenrente um freiwillige Angaben handelt. In dem Vordruck „Einkommenserklärung nach dem Bundesgesetz über den Abbau der Fehlsubventionierung im Wohnungswesen" wird daher künftig darauf hingewiesen, daß Angaben zu solchen Einkünften freiwillig sind, daß jedoch für den Fall, daß die übrigen Einkommen nicht zum Lebensunterhalt ausreichen, der Betroffene mit Rückfragen rechnen muß. Durch die freiwillige Angabe solcher Einkunftsarten kann eine solche Rückfrage möglicherweise vermieden werden.

Die Stadt hat außerdem vorgesehen, den Freiwilligkeitshinweis und entsprechende Erläuterungen bei einer neuen Drucklegung der Einkommenserklärungen im Bereich von Sozialwohnungen zu übernehmen.

8.7. Datenübermittlung Gemeinde – Amt für Landwirtschaft

Ein Amt für Landwirtschaft erbat von einer kreisangehörigen Gemeinde personenbezogene Angaben über bäuerliche forstwirtschaftliche Lohnunternehmer und über von diesen geleistete Gemeindearbeiten. Verwendungszweck beim Amt für Landwirtschaft sollte die Rechnungsprüfung zur Gasöl-Verbilligung sein, da die genannten Arbeiten im Gegensatz zu Forstarbeiten im land- und forstwirtschaftlichen Betrieb durch den Betrieb selbst nicht Gasöl-Verbilligungs-begünstigt sind. Zu klären war, ob die Gemeinde dem Wunsch des Amts für Landwirtschaft entsprechend außer Namen und Anschrift für bestimmte Kalenderjahre auch geleistete Arbeitsstunden, Leistung in fm/rm, Fuhrlohn je fm/rm und Gesamtfuhrlohn in DM übermitteln konnte.

Da die personenbezogenen Angaben bei der Gemeinde für Arbeiten im Gemeindewald und damit für einen ganz anderen Zweck, als die Rechnungsprüfung zur Gas-Öl-Verbilligung, beim Amt für Landwirtschaft entstanden waren, galt es festzustellen, ob die mit der Übermittlung verbundene Zweckänderung die Zulässigkeit der Übermittlung berührt. Eine Tätigkeit der Gemeinde „im Wettbewerb" entspr. Art. 22 BayDSG war dabei nicht anzunehmen. Ich habe den Sachverhalt folgendermaßen beurteilt:

Art. 17 BayDSG stellt für die Übermittlung personenbezogener Daten zwischen zwei öffentlichen Stellen darauf ab, ob sie für die „rechtmäßige" Erfüllung durch Rechtsnorm zugewiesener Aufgaben „erforderlich" ist. Nach § 6 Haushaltsgrundsätze-Gesetz und Art. 7 Bayer. Haushaltsordnung müssen staatliche Behörden die Grundsätze der Wirtschaftlichkeit und Sparsamkeit beachten. Eine entsprechende Aufgabenzuweisung beim Amt für Landwirtschaft war daher anzunehmen. Unter Berücksichtigung des Urteils des Bundesverfassungsgerichts vom 15.12.1983 halte ich bei Datenübermittlung öffentlicher Stellen im Rahmen der Prüfung, ob Daten zur „rechtmäßigen" Erfüllung „erforderlich" sind für geboten, eine Änderung des Nutzungszwecks der Daten, die mit der Übermittlung verbunden wäre, unter dem Gesichtspunkt der Verhältnismäßigkeit ihrer Auswirkungen auf den Betroffenen zu überprüfen.

Kriterien für die Anwendbarkeit des Verhältnismäßigkeitsgrundsatzes lassen sich hier aus einem ähnlichen gesetzlich bereits seit langem geregelten Fall herleiten: Das Auskunftsersuchen des Amtes für Landwirtschaft weist in seinem materiell-rechtlichen Gehalt erhebliche Ähnlichkeit mit dem Begehren einer Kontrollmitteilung durch das Finanzamt im Steuerrecht auf. Für das Besteuerungsverfahren hat nun § 93 Abs 1 der Abgabenordnung festgelegt, daß die Beteiligten und andere Personen der Finanzbehörde zur Feststellung eines für die Besteuerung erheblichen Sachverhalts die erforderlichen Auskünfte zu erteilen haben. Andere Personen als die Beteiligten selbst sollen aber nach § 93 Abs. 1 Satz 3 erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziele führt oder keinen Erfolg verspricht (siehe auch 6. Tätigkeitsbericht unter 4.8.2).

Entsprechend diesem Rechtsgedanken habe ich die Übermittlung von Name und Anschrift der Betroffenen durch die Gemeinde an das Amt für Landwirtschaft zur Erfüllung der genannten haushaltsrechtlichen Grundsätze für erforderlich und verhältnismäßig gehalten. Gegen die gleichzeitige Weiterleitung der übrigen Daten habe ich jedoch unter dem Gesichtspunkt der Verhältnismäßigkeit Bedenken erhoben, da sie der Gemeinde für einen ganz anderen Verwendungszweck bekannt wurden. Ich habe empfohlen, die anderen Angaben – mit Hilfe der übermittelnden Anschriften zunächst bei dem Betroffenen selbst zu erfragen.

8.8. Datenerhebung für das „Zeugnis über das Nichtbestehen eines Vorkaufsrechts"

Ein Grundbuchamt darf bei Kaufverträgen den Erwerber als Eigentümer nur dann in das Grundbuch eintragen, wenn die Nichtausübung oder das Nichtbestehen der gemeindlichen Vorkaufsrechte gemäß §§ 24 ff BBauG nachgewiesen wird (§ 24 Abs. 5 BBauG). Auf Antrag eines Beteiligten muß die Gemeinde daher unverzüglich ein entsprechendes Zeugnis ausstellen. Dabei kommt es offenbar gelegentlich vor, daß die Gemeinde vom Notar die Übersendung einer Vertragsabschrift verlangt und es ablehnt, vorher das erbetene Zeugnis zu erteilen.

Das OVG Münster hat in seiner Entscheidung vom 24. April 1979 (NJW 1980, 1067) dargestellt, daß die Gemeinde zumindest den Antrag auf ein Zeugnis über das Nichtbestehen eines Vorkaufsrechts nicht mit der Begründung ablehnen kann, der Grundstückseigentümer habe zuvor eine Abschrift des Kaufvertrages vorzulegen. Zu der Frage, ob ein Vorkaufsrecht besteht oder nicht muß sich die Gemeinde also äußern, auch ohne daß ihr eine vollständige Abschrift des Kaufvertrags vorliegt.

Der Präsident der Landesnotarkammer Bayern hat die bayerischen Notare hierauf hingewiesen und ausgeführt, daß die Vertragsbeteiligten aus Gründen der Geheimhaltung ihrer Rechtsgesschäfte und auch aus Kostengründen in aller Regel Wert darauf legen, daß Dritte von dem Inhalt des Kaufvertrages nur dann Kenntnis erhalten, wenn dies gesetzlich vorgeschrieben ist oder im Interesse der Vertragsteile liegt. Es erscheint der Landesnotarkammer Bayern daher notwendig, die Frage ob, der Gemeinde von vorneherein eine vollständige Vertragsabschrift übersandt werden soll oder erst dann, wenn die Gemeinde das Bestehen eines Vorkaufsrechts bestätigt hat, mit den Beteiligten unter Hinweis auf die Rechtslage ausdrücklich zu erörtern.

Ich unterstütze diese Ausführungen der Landesnotarkammer Bayern. Sie werden dem Gedanken des informationellen Selbstbestimmungsrechts sehr deutlich gerecht.

8.9. Auskunft über Anschriften von Familien mit nichtschulpflichtigen Kindern und mit Hunden an die Bundesbahn

Die Deutsche Bundesbahn hat von Gemeinden Anschriften von Familien mit nichtschulpflichtigen Kindern und mit Hunden erbeten. Da Angaben über Hundehalter nur aus Unterlagen über die Hundesteuer entnommen werden können, war eine entsprechende Datenübermittlung wegen des Steuergeheimnisses nicht möglich. Von allgemeinerem Interesse mag jedoch die Frge der Übermittlung von Anschriften von Familien mit nichtschulpflichtigen Kindern aus dem Melderegister sein: Hier war die Übermittlungsmöglichkeit nach Art. 31 und nach Art. 34 MeldeG zu prüfen.

Die Deutsche Bundesbahn ist zwar eine öffentliche Stelle. Man kann jedoch nicht davon ausgehen, daß die Datenübermittlung wie es Art. 31 Abs. 1 Satz 1 MeldeG verlangt, „zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich" ist. Die Erforderlichkeit zur Aufgabenerfüllung kann nämlich nicht angenommen werden, wenn die Übermittlung lediglich geeignet und zweckmäßig ist. Dies könnte im vorliegenden Fall zutreffen. Für „erforderlich" im Sinne des Meldegesetzes halte ich die Datenübermittlung dagegen nicht; denn andernfalls müßten allen öffentlichen Stellen, die zu anderen öffentlichen oder nichtöffentlichen Stellen mit ihren Leistungen im Wettbewerb stehen, Gruppenauskünfte aus dem Melderegister erteilt werden. Außerdem müßten aufgrund des Gleichbehandlungsgrundsatzes die gleichen Auskünfte dann auch nichtöffentlichen Mitbewerbern erteilt werden können.

Grundsätzlich wäre wohl auch möglich, die Bundesbahn, wenn sie im Wettbewerb auftritt, wie eine nichtöffentliche Stelle zu behandeln und die Möglichkeit einer Datenübermittlung nach Art. 34 Abs. 3 MeldeG zu prüfen. Danach darf jedoch die Gruppenauskunft nur erteilt werden, wenn sie im öffentlichen Interesse liegt. Ein solches ist in Fällen von Datenübermittlung für Vereine oder vorwiegend kommerzielle Interessen (z.B. Wahlwerbung, Mitgliederwerbung, Werbung für Dienstleistung o.ä. für wirtschaftliche Unternehmen und Verbände, beispielsweise Versicherungsunternehmen, Kreditinstitute) nicht anzunehmen; siehe auch Nr. 34.6 der Vollzugsbekanntmachung zum MeldeG (MABl 1984 Seite 177 ff, Seite 190). Die Datenübermittlung an die Deutsche Bundesbahn war daher auch nach Art. 34 Abs. 3 MeldeG nicht zulässig.

8.10. Namensnennung in öffentlicher Gemeinderatssitzung?

Ein Bürger hatte sich darüber beschwert, daß sein Name in der öffentlichen Gemeinderatssitzung über einen Bebauungsplan genannt wurde, gegen den er Einwendungen erhoben hatte. Die Gemeinde hatte mir dazu mitgeteilt, daß aus ihrer Sicht ein öffentliches Interesse an der Behandlung der Einwendungen in öffentlicher Sitzung bestanden habe.

Nach meiner Auffassung hat sich die Gemeinde damit nicht in Widerspruch zu datenschutzrechtlichen Vorschriften gesetzt. Nach Art. 52 Abs. 2 Satz 1 der Bayerischen Gemeindeordnung sind Sitzungen des Gemeinderates grundsätzlich öffentlich; ein Abweichen von diesem Grundsatz ist nur dann vorgesehen, wenn Rücksichten auf das Wohl der Allgemeinheit oder auf berechtigte Ansprüche Einzelner entgegenstehen. Ein solcher Anspruch eines Einzelnen konnte hier nicht angenommen werden. Durch die Nennung des Namens in einer öffentlichen Gemeinderatssitzung werden schutzwürdige Belange des Gemeindebürgers, der mit Rechtsbehelfen gegen gemeindliches Tun vorgeht, im Regelfall nicht unverhältnismäßig beeinträchtigt. Der Grundsatz der Öffentlichkeit von Gemeinderatssitzungen dient der Transparenz des gemeindlichen Handelns und ist letztlich ein Ausfluß des Demokratiegebots unserer Verfassung. Im gemeindlichen Bereich soll es sicherstellen, daß die Gemeindebürger in der Lage sind, die Behandlung der Anliegen von Mitbürgern durch die Gemeinde auch zu kontrollieren.

8.11. Nennung der Privatanschriften von Bauantragstellern in öffentlicher Sitzung und in Protokollen des Bauausschusses

Aufgrund des Antrags eines Bürgers hatte ich mich mit der Frage auseinanderzusetzen, inwieweit Privatanschriften von Bauantragstellern in öffentlicher Bauausschußsitzung genannt und in Protokollen über diese Sitzungen wiedergegeben werden dürfen.

In diesem Zusammenhang ist zunächst auf die Vorschrift des Art. 84 der Bayerischen Bauordnung (BayBO) hinzuweisen, nach der Bauaufsichtsbehörden und Gemeinden Ort und Straße der Baustelle, Art und Größe des Bauvorhabens sowie Namen und Anschrift des Bauherrn und des Entwurfsverfassers nur veröffentlichen oder an Dritte zum Zweck der Veröffentlichung übermitteln dürfen, wenn der Betroffene der Veröffentlichung nicht widersprochen hat. Der Betroffene ist bei der Bauantragstellung auf sein

Widerspruchsrecht hinzuweisen. Nach dieser Vorschrift verdienen also die genannten Daten Schutz vor unbefugter Nutzung durch Dritte. Dieser Gedanke ist meines Erachtens im Hinblick auf das informationelle Selbstbestimmungsrecht in einer öffentlichen Gemeinderats- oder Bauausschußsitzung insoweit zu berücksichtigen, daß es unverhältnismäßig und daher nicht zulässig wäre, zu jedem aufgerufenen Tagesordnungspunkt routinemäßig – ohne besondere Notwendigkeit im Einzelfall – Privatanschriften von Bauwerbern bekanntzugeben. Der Schutzgedanke aus Art. 84 BayBO kann jedoch nicht so aufgefaßt werden, daß den Mitgliedern des Gremiums bzw. der Verwaltung verboten wäre, im Zuge der Debatte über einen Antrag bestimmte in Art. 84 genannte Angaben in der öffentlichen Sitzung erforderlichenfalls zu nennen. Dementsprechend würde ein Protokoll, das nur Erörtertes und Bekanntgegebenes widergibt, im Ergebnis nur selten Privatanschriften von Bauwerbern enthalten.

Nach Art. 54 Abs. 3 Satz 2 der Bayerischen Gemeindeordnung (BayGO) steht die Einsicht in die Niederschriften über öffentliche Sitzung allen Gemeindebürgern frei. Gemäß Art. 55 Abs. 2 BayGO gilt dies auch für den Bauausschuß. Beschränkt ist das Recht auf Einsichtnahme allerdings auf Gemeindebürger und auf Niederschriften öffentlicher Sitzungen. Der Inhalt der Niederschrift über eine öffentliche Sitzung bestimmt sich in Art. 54 BayGO. Die Sitzungsniederschrift ist eine öffentliche Urkunde im Sinne von § 415 ZPO, die grundsätzlich den wesentlichen Inhalt der Beratung und Beschlußfassung wiedergeben soll. Ein Protokoll darf danach die vollen Privatanschriften der jeweiligen Bauwerber nur wiedergeben, wenn sie in der Sitzung des Bauausschusses genannt wurden (siehe oben). Eine Einsichtnahme eines Gemeindebürgers in ein Protokoll, das die Privatanschriften der Bauwerber enthielte, obwohl diese in der Sitzung nicht genannt wurden, ist grundsätzlich geeignet die betroffenen Bauwerber in ihren schutzwürdigen Belangen zu beeinträchtigen. Soweit Protokolle insofern unrichtig sind, müssen sie daher vor Einsichtgewährung durch Schwärzung der entsprechenden Daten berichtigt werden.

Soweit die Anschriften der Bauwerber jedoch in der Sitzung genannt wurden und dies die Protokolle auch ausweisen, sind sie korrekt. Ob eine Einsichtnahme eines Dritten in diese Protokolle geeignet wäre schutzwürdige Belange des Betroffenen zu beeinträchtigen, muß dabei dahinstehen, denn das Recht auf Einsichtnahme bestimmt sich ausschließlich nach Art. 54 Abs. 3 GO. Danach hat der Gesetzgeber eine Abwägung zwischen schutzwürdigen Belangen Einzelner und dem berechtigten Interesse an einer Einsichtnahme durch Beschränkung des Einsichtsrechts auf Gemeindebürger und auf korrekte Niederschriften über öffentliche Sitzungen bereits vorweggenommen.

Allerdings umfaßt das Recht auf Einsicht nach Art. 54 Abs. 3 Satz 2 BayGO meines Erachtens keinen Anspruch auf Herstellung von Abschriften und Ablichtungen. Dies folgt aus dem Umkehrschluß zu Art. 54 Abs. 3 Satz 1 BayGO, der Gemeinderatsmitgliedern neben dem Recht auf Einsicht ausdrücklich das Recht gewährt, sich Abschriften der in öffentlicher Sitzung gefaßten Beschlüsse erteilen zu lassen.

Dieser Sachverhalt ist aus der Sicht des Datenschutzes deswegen interessant, weil die Anschriften der Bauwerber im Adreßhandel einen gewissen Marktwert haben.

8.12. Umgang mit Gewerbetreibenden-Daten

1982 hatte ich dem Bayer. Staatsministerium für Wirtschaft und Verkehr Änderungsvorschläge für Auskünfte bzw. Datenübermittlungen aus den Gewerbekarteien unterbreitet und die Schaffung einer bereichsspezifischen Rechtsgrundlage gefordert, um bestehende Diskrepanzen zwischen Gewerbe- und Melderecht zu beseitigen (s. V. Tätigkeitsbericht, Nr. 4.14, S. 52).

Parallel dazu lief eine Initiative des Bundeswirtschaftsministers u.a. zur Regelung der Datenübermittlungen aus den Gewerbekarteien durch Anfügung eines 5. Absatzes an § 14 der Gewerbeordnung. Der Vorschlag, der auch auf Kritik der Datenschutzbeauftragten des Bundes und der Länder gestoßen war, wurde schließlich nach Erlaß des Volkszählungsurteils vom 15.12.1983 zurückgezogen.

Das Bayer. Staatsministerium für Wirtschaft und Verkehr hat daraufhin wiederholt seine Bereitschaft erklärt, entsprechende Vorschläge für bereichsspezifische Gewerbedaten-Übermittlungsvorschriften zu unterstützen, sobald die Auswirkungen des Volkszählungsurteils auf die Verarbeitung (insbesondere Datenübermittlung) von Gewerbetreibendendaten umgesetzt werden könnten. Da es sich um „zwangsweise" erhobene Daten handelt, auf die sich das Volkszählungsurteil des BVerfG unstreitig bezieht, sollte dieses Thema alsbald in Angriff genommen werden.

9. Einwohnermelderegister

9.1. Wahlwerbung mit Meldedaten

Wie schon im 6. Tätigkeitsbericht näher dargelegt, gingen beim Landesbeauftragten für den Datenschutz vor der Kommunalwahl 1984 wiederum eine größere Anzahl von Beschwerden wegen Nutzung von Meldedaten durch Parteien ein. Den Betroffenen war jeweils unbekannt, daß sie der Weitergabe ihrer Anschrift an Parteien zu Wahlwerbezwecken hätten widersprechen können (Art. 35 Abs. 1 Satz 3 MeldeG). Dies ist nicht verwunderlich, da weder das Meldegesetz noch die Vollzugsbekanntmachung zum Meldegesetz vorsehen, daß von seiten der Meldebehörden auf dieses Widerspruchsrecht öffentlich hinzuweisen sei. Gleichwohl habe ich entsprechende Bekanntmachungen immer wieder angeregt (siehe 6. Tätigkeitsbericht Nr. 4.7.16 Seite 53/54).

9.2. Veröffentlichung von Geburten, Eheschließungen und Sterbefällen

In Eingaben wird die Zulässigkeit der Veröffentlichung von Geburten, Eheschließungen oder Sterbefällen gelegentlich in Zweifel gezogen. Auch die zuständigen Behörden erkundigen sich hierzu gelegentlich nach der Rechtslage. Insgesamt scheinen mir dabei diejenigen, die solche Veröffentlichungen ablehnen, sehr selten zu sein. Die überwiegende Mehrheit hält es mit Witwe Marthe Schwerdtlein – anläßlich des Todes ihres Mannes –: „... möcht ihn auch tot im Wochenblättchen lesen" (Goethe, Faust I)

Die Weitergabe von Daten über Geburten, Eheschließungen und Sterbefälle von den Standesämtern an die Presse setzte bisher nach der ausdrücklichen Regelung in § 104 der Dienstanweisung für die Standesbeamten und deren Aufsichtsbehörden (DA) die vorherige schriftliche Einwilligung der Beteiligten mit entsprechender Belehrung über die Bedeutung und Folgen einer Veröffentlichung voraus. Als Folge einer Änderung der DA ist § 104 nun weggefallen. Gleichwohl bleibt meines Erachtens die Rechtslage insofern unverändert, als die genannten Daten nach wie vor an die Presse zur Veröffentlichung weitergegeben werden können, soweit entsprechende Einwilligungen der Beteiligten (nach Aufklärung über Folgen der Einwilligung) vorliegen. Dies ergibt sich für Daten, die in einer Datei gespeichert sind, aus Art. 4 Abs. 1 Nr. 2 BayDSG wonach eine Übermittlung stets zulässig ist, wenn der Betroffene eingewilligt hat. Dieser Grundsatz gilt aber grundsätzlich auch für Übermittlungen aus anderen Unterlagen als Dateien – jedenfalls soweit keine entgegenstehenden Vorschriften dies ausdrücklich anders regeln. Der Wegfall von § 104 DA berührt mithin zwar nicht die datenschutzrechtliche Bewertung, wohl aber die Frage, inwieweit die Gemeinde gehalten ist, für Veröffentlichungen Vorsorge zu tragen.

9.3. Zum Verhältnis Hotelgast/Meldebehörde

Eine bayerische Gemeinde hatte von sich aus regelmäßig Listen mit Daten der Gäste von Beherbergungsbetrieben an die Polizei übersandt. Damit änderte die Gemeinde die vom Meldegesetz vorgesehene Verfahrensweise: Nach Art. 27 Abs. 4 und Art. 29 Abs. 1 des Bayerischen Meldegesetzes müssen sich Gäste gerade nicht bei der Meldebehörde melden. Die Gemeinde erhält, außer eventuell für Zwecke des Kurbeitrags, keine namentliche Übersicht über Hotelgäste. Diese Regelung wurde in erster Linie im Interesse der Gäste und der Beherbergungsbetriebe getroffen. Sie dient damit aber auch der Gemeinde, weil Gäste sich im Urlaub möglichst frei und ungezwungen fühlen sollen und sich nur im unumgänglich nötigen Umfang behördlich beobachtet sehen wollen.

Die Polizei ihrerseits darf nach Art. 27 Abs. 4 MeldeG die Aushändigung der Beherbergungsmeldescheine nur bei den Beherbergungsstätten selbst verlangen. Diese Meldescheine dürfen von der Polizei nach Art 29 Abs. 1 Satz 1 MeldeG ausgewertet und verarbeitet werden, soweit dies zur rechtmäßigen Aufgabenerfüllung erforderlich ist. Sofern nicht aufgrund besonderer Umstände im Einzelfalle etwas anderes gilt, werden der Polizei stichprobenartige Überprüfungen bei den Beherbergungsstätten genügen.

Neben dem vorgenannten polizeilichen Zweck dürfen die Beherbergungsmeldescheine, die bei den Beherbergungsbetrieben anfallen, wie erwähnt, nur durch die Gemeinde zur Festsetzung des Kurbeitrags ausgewertet und verarbeitet werden. Die Nutzungsbeschränkung auf die Kurbeitragsfeststetzung schließt eine Übermittlung von Gästelisten von der Gemeinde an die Polizei aus.

9.4. Bayerische Meldedaten-Übermittlungsverordnung (BayMeldeDÜV) nach Art. 31 Abs. 5 MeldeG

Zum 1. Januar 1985 trat die BayMeldeDÜV in Kraft. Einige grundsätzliche Bedenken gegen darin vorgesehene Regelungen hatte ich bereits in meinem 6. Tätigkeitsbericht dargestellt (Nr. 4.7.5, Seite 50). Vor Erlaß der Verordnung habe ich noch auf folgende mir problematisch erscheinende Punkte hingewiesen:

a) Zum Begriff „regelmäßige Datenübermittlung":

Der Begriff „regelmäßige Datenübermittlung" wird in der MeldeDÜV sehr restriktiv ausgelegt. Im Sinne der Durchschaubarkeit automatischer Datenverarbeitung für die Betroffenen – deren Daten weiter übermittelt werden – hätte ich dagegen eine Offenlegung von weit mehr Übermittlungsfällen in der Verordnung für angezeigt gehalten: Ich hatte die Ansicht vertreten, daß die BayMeldeDÜV nicht nur Datenübermittlungen ausweisen sollte, die dann erfolgen, wenn sich im Datenbestand fallbezogen etwas ändert (z.B. bei Zuzug, Wegzug, Änderung des Familienstandes). Vielmehr sollten auch solche Übermittlungen in der BayMeldeDÜV ausgewiesen sein, die sonst zwischen Datenempfängern und Meldebehörde so festgelegt sind, daß die Übermittlungen gewissermaßen „programmiert" abgewickelt werden, also ohne daß die Meldebehörde vor der Übermittlung nochmals eine Entscheidung trifft, bei der sie die Erforderlichkeit der Datenübermittlung zur Erfüllung von Aufgaben des Empfängers prüfen könnte, bei denen also Daten nur vom Empfänger „abgerufen" werden. Dem ist mit dem Argument, daß dies zu einer starken Ausweitung der Verordnung geführt hätte, nicht gefolgt worden.

b) Zur verbindlichen Einführung bestimmter Datenformate:

Die BayMeldeDÜV (wie auch die Datenübermittlungsverordnungen des Bundes) binden die Meldebehörden an den „Datensatz für das Meldewesen". Dadurch wird eine Vereinheitlichung der Art der Darstellung der einzelnen Daten (Datenformate) nicht nur bei den Meldebehörden, sondern auch bei den Stellen erreicht, die Empfänger regelmäßiger Datenübermittlungen sind oder werden. Damit wird eine allgemeine einheitliche Struktur der Datenverarbeitung gefördert, die das Verknüpfen von Datenbeständen erleichert, die bisher getrennt voneinander verwaltet werden. Dies kann sich als problematisch erweisen, weil es die Herstellung von Datenprofilen Einzelner erleichtert, die, je nach Umfang, das Persönlichkeitsrecht stark berühren können.

c) Übermittlung von Daten Deutscher an Ausländerbehörden:

Gegen die regelmäßige Übermittlung von Daten Deutscher an die Ausländerbehörden, die zugleich eine fremde Staatsangehörigkeit besitzen, habe ich wiederholt Bedenken erhoben. Da hierüber gegenwärtig beim Bayerischen Verfassungsgericht auch eine Verfassungsbeschwerde anhängig ist, stelle ich weitere Ausführungen zu diesem Thema zurück.

d) künftige Nutzung von Melderegistern im AKDB-Verbund durch Ausländerbehörden

Widerspruchsrecht hinzuweisen. Nach dieser Vorschrift verdienen also die genannten Daten Schutz vor unbefugter Nutzung durch Dritte. Dieser Gedanke ist meines Erachtens im Hinblick auf das informationelle Selbstbestimmungsrecht in einer öffentlichen Gemeinderats- oder Bauausschußsitzung insoweit zu berücksichtigen, daß es unverhältnismäßig und daher nicht zulässig wäre, zu jedem aufgerufenen Tagesordnungspunkt routinemäßig – ohne besondere Notwendigkeit im Einzelfall – Privatanschriften von Bauwerbern bekanntzugeben. Der Schutzgedanke aus Art. 84 BayBO kann jedoch nicht so aufgefaßt werden, daß den Mitgliedern des Gremiums bzw. der Verwaltung verboten wäre, im Zuge der Debatte über einen Antrag bestimmte in Art. 84 genannte Angaben in der öffentlichen Sitzung erforderlichenfalls zu nennen. Dementsprechend würde ein Protokoll, das nur Erörtertes und Bekanntgegebenes widergibt, im Ergebnis nur selten Privatanschriften von Bauwerbern enthalten.

Nach Art. 54 Abs. 3 Satz 2 der Bayerischen Gemeindeordnung (BayGO) steht die Einsicht in die Niederschriften über öffentliche Sitzung allen Gemeindebürgern frei. Gemäß Art. 55 Abs. 2 BayGO gilt dies auch für den Bauausschuß. Beschränkt ist das Recht auf Einsichtnahme allerdings auf Gemeindebürger und auf Niederschriften öffentlicher Sitzungen. Der Inhalt der Niederschrift über eine öffentliche Sitzung bestimmt sich in Art. 54 BayGO. Die Sitzungsniederschrift ist eine öffentliche Urkunde im Sinne von § 415 ZPO, die grundsätzlich den wesentlichen Inhalt der Beratung und Beschlußfassung wiedergeben soll. Ein Protokoll darf danach die vollen Privatanschriften der jeweiligen Bauwerber nur wiedergeben, wenn sie in der Sitzung des Bauausschusses genannt wurden (siehe oben). Eine Einsichtnahme eines Gemeindebürgers in ein Protokoll, das die Privatanschriften der Bauwerber enthielte, obwohl diese in der Sitzung nicht genannt wurden, ist grundsätzlich geeignet die betroffenen Bauwerber in ihren schutzwürdigen Belangen zu beeinträchtigen. Soweit Protokolle insofern unrichtig sind, müssen sie daher vor Einsichtgewährung durch Schwärzung der entsprechenden Daten berichtigt werden.

Soweit die Anschriften der Bauwerber jedoch in der Sitzung genannt wurden und dies die Protokolle auch ausweisen, sind sie korrekt. Ob eine Einsichtnahme eines Dritten in diese Protokolle geeignet wäre schutzwürdige Belange des Betroffenen zu beeinträchtigen, muß dabei dahinstehen, denn das Recht auf Einsichtnahme bestimmt sich ausschließlich nach Art. 54 Abs. 3 GO. Danach hat der Gesetzgeber eine Abwägung zwischen schutzwürdigen Belangen Einzelner und dem berechtigten Interesse an einer Einsichtnahme durch Beschränkung des Einsichtsrechts auf Gemeindebürger und auf korrekte Niederschriften über öffentliche Sitzungen bereits vorweggenommen.

Allerdings umfaßt das Recht auf Einsicht nach Art. 54 Abs. 3 Satz 2 BayGO meines Erachtens keinen Anspruch auf Herstellung von Abschriften und Ablichtungen. Dies folgt aus dem Umkehrschluß zu Art. 54 Abs. 3 Satz 1 BayGO, der Gemeinderatsmitgliedern neben dem Recht auf Einsicht ausdrücklich das Recht gewährt, sich Abschriften der in öffentlicher Sitzung gefaßten Beschlüsse erteilen zu lassen.

Dieser Sachverhalt ist aus der Sicht des Datenschutzes deswegen interessant, weil die Anschriften der Bauwerber im Adreßhandel einen gewissen Marktwert haben.

8.12. Umgang mit Gewerbetreibenden-Daten

1982 hatte ich dem Bayer. Staatsministerium für Wirtschaft und Verkehr Änderungsvorschläge für Auskünfte bzw. Datenübermittlungen aus den Gewerbekarteien unterbreitet und die Schaffung einer bereichsspezifischen Rechtsgrundlage gefordert, um bestehende Diskrepanzen zwischen Gewerbe- und Melderecht zu beseitigen (s. V. Tätigkeitsbericht, Nr. 4.14, S. 52).

Parallel dazu lief eine Initiative des Bundeswirtschaftsministers u.a. zur Regelung der Datenübermittlungen aus den Gewerbekarteien durch Anfügung eines 5. Absatzes an § 14 der Gewerbeordnung. Der Vorschlag, der auch auf Kritik der Datenschutzbeauftragten des Bundes und der Länder gestoßen war, wurde schließlich nach Erlaß des Volkszählungsurteils vom 15.12.1983 zurückgezogen.

Das Bayer. Staatsministerium für Wirtschaft und Verkehr hat daraufhin wiederholt seine Bereitschaft erklärt, entsprechende Vorschläge für bereichsspezifische Gewerbedaten-Übermittlungsvorschriften zu unterstützen, sobald die Auswirkungen des Volkszählungsurteils auf die Verarbeitung (insbesondere Datenübermittlung) von Gewerbetreibendendaten umgesetzt werden könnten. Da es sich um „zwangsweise" erhobene Daten handelt, auf die sich das Volkszählungsurteil des BVerfG unstreitig bezieht, sollte dieses Thema alsbald in Angriff genommen werden.

9. Einwohnermelderegister

9.1. Wahlwerbung mit Meldedaten

Wie schon im 6. Tätigkeitsbericht näher dargelegt, gingen beim Landesbeauftragten für den Datenschutz vor der Kommunalwahl 1984 wiederum eine größere Anzahl von Beschwerden wegen Nutzung von Meldedaten durch Parteien ein. Den Betroffenen war jeweils unbekannt, daß sie der Weitergabe ihrer Anschrift an Parteien zu Wahlwerbezwecken hätten widersprechen können (Art. 35 Abs. 1 Satz 3 MeldeG). Dies ist nicht verwunderlich, da weder das Meldegesetz noch die Vollzugsbekanntmachung zum Meldegesetz vorsehen, daß von seiten der Meldebehörden auf dieses Widerspruchsrecht öffentlich hinzuweisen sei. Gleichwohl habe ich entsprechende Bekanntmachungen immer wieder angeregt (siehe 6. Tätigkeitsbericht Nr. 4.7.16 Seite 53/54).

9.2. Veröffentlichung von Geburten, Eheschließungen und Sterbefällen

In Eingaben wird die Zulässigkeit der Veröffentlichung von Geburten, Eheschließungen oder Sterbefällen gelegentlich in Zweifel gezogen. Auch die zuständigen Behörden erkundigen sich hierzu gelegentlich nach der Rechtslage. Insgesamt scheinen mir dabei diejenigen, die solche Veröffentlichungen ablehnen, sehr selten zu sein. Die überwiegende Mehrheit hält es mit Witwe Marthe Schwerdtlein – anläßlich des Todes ihres Mannes –: „... möcht ihn auch tot im Wochenblättchen lesen" (Goethe, Faust I)

Gemeinde enthalten, sondern sich statt dessen auf den Datenbestand des ganzen Landkreises oder Regierungsbezirkes beziehen, der Fall. Noch deutlicher würde sich das Problem zeigen, wenn (was nicht der Fall ist) alle Bayerischen Melderegister in einer einzigen Datenbank gemeinsam gespeichert würden. Dies käme einem landeszentralen Einwohnerregister gleich, das anstelle von über 1200 gemeindlichen Melderegistern technisch verfügbar wäre. Ich stütze meine Rechtsansicht hierzu – wie oben erwähnt – darauf, daß das Meldegesetz solche Abfragen nicht vorsieht, den Meldebehörden selbst dieses Recht nach dem Meldegesetz nicht zustände und die bezeichneten weitergehenden Nutzungen überdies einen erheblichen schweren Eingriff darstellen würden, der nicht entsprechend besonders legitimiert wäre.

Dieser Rechtsansicht dürften auch nicht wesentliche Bedürfnisse der polizeilichen Praxis entgegenstehen. Denn eine solche, über die einzelnen Meldebehörden hinausgreifende Möglichkeit zur Nutzung der Meldedaten stand der Polizei im bisherigen Verfahren nicht zur Verfügung. So würde bereits ein Online-Anschluß an jeweils einzelne Melderegister in dem oben (s. unter f) für zulässig erachteten Rahmen eine erhebliche Erleichterung der polizeilichen Arbeit darstellen. Dies gilt zumal, wenn über den Anschluß an die in einer gemeinsamen Datenbank betriebenen Melderegister vieler Gemeinden einzelnen Polizeidienststellen der Abruf von Meldedaten einer Vielzahl von Meldebehörden ermöglicht wird. Deshalb müßte angesichts dieser deutlichen Erleichterung beim Zugang zu Meldedaten auch unter dem Gesichtspunkt polizeilicher Bedürfnisse – von der Rechtsfrage der Zulässigkeit abgesehen – der Verzicht auf Abruf aus den gesamten jeweils bei den Rechenzentren der AKDB gespeicherte Meldedatenbeständen hinnehmbar sein.

Auch durch technische und organisatorische Maßnahmen muß sichergestellt werden, daß die Meldebehörden an Polizeidienststellen nur „Daten ihrer Melderegister" übermitteln. D. h. – nach Auffassung des Landesbeauftragten für den Datenschutz – daß auch technisch nicht die Voraussetzungen dafür geschaffen werden dürfen, durch den gemeinsamen Betrieb von Melderegistern in einer Datenbank erst entstehende Nutzungsmöglichkeiten durch die Polizei in Anspruch zu nehmen.

In der vom Staatsministerium des Innern nach § 8 Abs. 2 vorzunehmenden Festlegung von Art und Umfang der Abfrage muß die auf die einzelne Meldebehörde (i.d. Regel Gemeinde) begrenzte Abfragemöglichkeit durch Polizeidienststellen eindeutig geregelt werden.

10. Steuerverwaltung

10.1. Braucht das Finanzamt Krankheitsdiagnosen?

Aus einem anderen Bundesland wurde ich darauf aufmerksam gemacht, daß Finanzverwaltungen in einer großen Zahl von Fällen von Steuerbürgern ärztliche bzw. amtsärztliche Atteste, Bescheinigungen, Rechnungen ect. verlangen würden. Dabei werde in der Regel gefordert, daß die Bescheinigungen eine ärztliche Diagnose enthielten. Ich habe deshalb das Bayerische Staatsministerium der Finanzen gebeten zu der Frage Stellung zu nehmen, ob für die z.B. im Einkommensteuerrecht festgelegten Zwecke die vorzulegenden Bescheinigungen eine ausführliche ärztliche Diagnose enthalten müssen, oder ob es genügen könnte, sich auf Angaben wie „Notwendigkeit einer Kur" oder „Höhe der Erwerbsminderung" zu beschränken und auf die Begründung im einzelnen zu verzichten.

Das Bayerische Staatsministerium der Finanzen hat dazu mitgeteilt, es gehe in diesen Fällen weniger um das Abfragen persönlicher Daten, sondern um das Geltendmachen persönlicher Umstände durch den Steuerpflichtigen selbst, die er dann auch nachweisen müsse. Es bestehe kein Anlaß zur Annahme, daß die Finanzämter über das notwendige Maß hinaus Nachweise verlangten. Ein genereller Verzicht auf ärztliche Diagnosen könne aber nicht in Betracht kommen, weil die Nachweismöglichkeiten der Steuerpflichtigen nicht eingeschränkt werden dürften und außerdem mehr Gefälligkeitsatteste zu befürchten seien. Die Frage, welche Anforderungen an den Nachweis einer Erkrankung zu stellen seien, können nur nach der jeweils in Betracht kommenden Vorschrift und den hierzu gegebenfalls bestehenden Nachweisregelungen beantwortet werden. Soweit die maßgeblichen Rechts- und Verwaltungsvorschriften die Vorlage von Ausweisen, Bescheinigungen und Bescheiden – ohne eine auch nur allgemeine Krankheitsbezeichnung – vorsehen bzw. zulassen, ergäben sich ohnehin keine Schwierigkeiten. In den übrigen Fällen werde der Sache nach meist eine zumindest allgemeine Krankheitsbezeichnung erforderlich sein, schon um die notwendigen Grenzziehungen vorzunehmen und der Gefahr von Mißbräuchen Einhalt zu bieten. Einzelheiten der ärztlichen Diagnose würden dagegen für die zu beurteilenden Steuerfragen meist ohne Bedeutung sein. Es bleibe deshalb regelmäßig den Steuerpflichtigen überlassen, ob sie diesbezügliche ärztliche Feststellungen den Finanzbehörden übermitteln. Insoweit beständen daher gegen ein Unkenntlichmachen von Einzelheiten der ärztlichen Diagnose unter dem Gesichtspunkt der Erforderlichkeit keine Bedenken. Sofern die Verwaltung im Einzelfall nähere Angaben für erforderlich halten sollte, werde sie dieses Verlangen zu begründen haben.

10.2. Bekanntgabe von Steuerschulden durch Finanzämter in Pfändungsverfügungen

Wenn ein Finanzamt mit einer Pfändungsverfügung bei einem Dritten (sogenannter „Drittschuldner") Beträge pfändet, um Steuerschulden einzutreiben, erfährt der Dritte nach der gegenwärtigen Rechtslage, welche Steuern für welchen Zeitraum der Vollstreckungsschuldner dem Finanzamt schuldet. Denn nach § 260 Abgabenordnung (AO) ist „in der Pfändungsverfügung (§ 309 AO) für die beizutreibenden Geldbeträge der Schuldgrund anzugeben". Eine Verletzung des Steuergeheimnisses liegt wegen dieser ausdrücklichen gesetzlichen Regelung nicht vor (§ 30 Abs. 4 Nr. 2 AO). Da aber der Drittschuldner nicht gehindert ist, die Informationen aus der Pfändungsverfügung anderen Personen mitzuteilen, soll nach ständiger Rechtsprechung des Bundesfinanzhofs eine restriktive Information des Drittschuldners durch das Finanzamt erfolgen (BFH, Bundessteuerblatt 1957 Seite 80, 1964 Seite 22, vergl. VBl. Kommentar Tipke-Kruse zu § 260 AO, Tz. 4).

Um der Rechtsprechung des höchsten Finanzgerichts zu entsprechen, sowie wohl auch auf Drängen der Landes- und des Bundesbeauftragten für den Datenschutz, wurde im Steuerbereinigungsgesetz – Entwurf 1985 – vorgesehen, den § 309 AO in Abs. 2 zu ergänzen. Danach soll die Pfändungsverfügung einem Drittschuldner künftig „den beizutreibenden Geldbetrag nur in einer Summe, ohne Angabe der Steuerart und der Zeiträume für die er geschuldet wird, bezeichnen". Dadurch soll verhindert werden, daß Drittschuldnern Geschäfts-, Einkommens- oder Vermögensverhältnisse des Vollstreckungsschuldners bekannt werden. Die Novellierung der AO ist derzeit aber zurückgestellt und dem Steuerbereinigungsgesetz 1986 vorbehalten worden.

10.3. Versand von Steuerbescheiden und Steuererklärungsvordrucken

Ein Petent hatte Kritik daran geübt, daß ein Steuerbescheid mit den vielen schützenswerten Angaben, die er enthält, lediglich in verschlossenem Umschlag zugesandt werde. Ich habe mich jedoch auf den Standpunkt gestellt, daß die Versendung von Steuerbescheiden im verschlossenen Umschlag per Post grundsätzlich als ausreichende Sicherung von unbefugter Kenntnisnahme angesehen werden kann. Der Inhalt eines verschlossenen Umschlags steht unter dem grundrechtlichen Schutz des in Art. 10 Abs. 1 des Grundgesetzes geregelten Briefgeheimnisses, dessen Verletzung in § 202 des Strafgesetzbuches mit Strafe bedroht ist. Im Bereich der Post ist das Postgut durch die Verschwiegenheitspflicht der Postbediensteten als Amtsträger geschützt, deren Verletzung ebenfalls strafbar ist. Es liegen gegenwärtig keine Erkenntnisse vor, aus denen sich ergäbe, daß die Versendung im verschlossenen Umschlag durch die Post keinen ausreichenden Schutz vor unbefugter Kenntnisnahme durch Dritte darstellen würde. Angesichts der Menge der zu versendenen Steuerbescheide und den mit den speziellen Versendungsformen der Post verbundenen Kosten, halte ich die Versendung des Steuerbescheides im verschlossenen Umschlag als Standardbrief unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit für angemessen. Nach Art. 15 Abs. 1 Satz 2 BayDSG sind zur technischen und organisatorischen Sicherung von Daten gegen unbefugte Kenntnisnahme nur solche Maßnahmen erforderlich, die in ihrem Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen.

Ein anderer Petent beschwerte sich wegen der Übersendung der Steuererklärungsvordrucke im unverschlossenen Umschlag. Auch diese Versendungsart habe ich jedoch für ausreichend gehalten, da außer Namen und Anschrift sowie Steuernummer keine weiteren Daten über den Steuerpflichtigen in der Sendung enthalten sind. Die Steuernummer ist zudem nicht im Sichtfeld des Fenster-Kuverts angeordnet. Die Versendung in einem verschlossenen Umschlag mit der Folge der erhöhten Portokosten erschien mir angesichts der genannten Daten, die auch wenig aussagekräftig sind und eine Mißbrauchmöglichkeit im Regelfall nicht eröffnen, unangemessen.

10.4. Welche Angaben auf Steuererhebungs-Formularen sind „Pflicht" – welche sind freiwillig?

Die bisher verwendeten Formulare für den Antrag auf Lohnsteuerermäßigung, auf Lohnsteuerjahresausgleich sowie für die Einkommensteuererklärung enthalten den Hinweis: „Nach den Vorschriften der Datenschutzgesetze wird darauf hingewiesen, daß die mit der Steuererklärung angeforderten Daten aufgrund der §§ 149 ff der Abgabenordnung und des § 39a Abs. 2 des Einkommensteuergesetzes erhoben werden".

Dieser Hinweis genügt jedoch nicht voll den Anforderungen des Art. 16 Abs. 2 BayDSG: Danach ist der Betroffene, wenn Daten aufgrund einer Rechtsvorschrift bei ihm erhoben werden, auf diese Rechtsvorschrift, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Nach der erläuternden Vollzugsbekanntmachung zu Art. 16 BayDSG gilt dies auch, wenn Daten für die Bearbeitung eines Antrags der Betroffenen benötigt werden. Dort heißt es: „Besteht keine Rechtsvorschrift, die den Betroffenen zur Angabe verpflichtet, so genügt in diesen Fällen jedoch der Hinweis, daß ohne die geforderten Angaben die Bearbeitung des Antrags nicht möglich ist. Werden in den genannten Fällen Angaben gefordert, die für die Bearbeitung des Antrags nicht erforderlich sind, ist gemäß Nr. 16.4 auf die Freiwilligkeit der Angaben hinzuweisen" (Nr. 16.4.1 der VollzBekBayDSG). Die auf den Steuererklärungsformularen anzugebenden Daten werden nun teilweise nicht aufgrund einer gesetzlichen Vorschrift angefordert; der Betroffene macht sie in bestimmten Fällen vielmehr freiwillig (Lohnsteuerermäßigungsantrag, Lohnsteuerjahresausgleich). Die Formulare müßten deshalb um präzisere Hinweise ergänzt werden, die zwischen freiwilligen und Pflicht-Angaben unterscheiden bzw. die wesentlichen Vorschriften angeben, zu deren Vollzug sie benötigt werden. Außerdem müßte ein Hinweis darauf aufgenommen werden, daß Angaben über Dritte (Arbeitgeber, volljährige Kinder, Empfänger von privaten Rentenzahlungen, unterstützte bedürftige Personen) im Rahmen des Besteuerungsverfahrens auch gegen diese Personen verwendet werden dürfen (§ 85 ff AO).

Ich habe wegen der genannten Fragen das Bayerische Staatsministerium der Finanzen eingeschaltet. Es hat den für die Änderung der Vordrucke zuständigen Bundesminister der Finanzen davon unterrichtet und mitgeteilt, daß eine ggf. erforderliche Änderung des datenschutzrechtlichen Hinweises frühestens im Antragsvordruck für 1986 erfolgen könne. Die Angelegenheit ist noch nicht abgeschlossen.

11. Personalwesen

11.1. Datenschutz bei Beihilfedaten

Zur Problematik verweise ich auf die ausführliche Darstellung meiner Ansicht im 6. Tätigkeitsbericht unter Nr. 4.9.1 Seiten 55 – 57. Im Berichtsjahr wurde vom Staatsministerium der Finanzen ein Entwurf einer gemeinsamen Bekanntmachung zum Persönlichkeitsschutz bei Beihilfedaten ausgearbeitet. Der Normprüfungsausschuß, dem der Entwurf vorgelegt wurde, hat jedoch auf seiner Sitzung am 26.9.1984 entschieden, daß eine gemeinsame Bekanntmachung nicht

erforderlich sei. Das Regelungsbedürfnis sei zwar grundsätzlich anzuerkennen, es solle jedoch nicht die Form einer gemeinsamen Bekanntmachung gewählt werden. Vielmehr solle jedes einzelne Ressort für seinen Geschäftsbereich eine nicht veröffentlichte Verwaltungsvorschrift (Ministerialrundschreiben) erlassen. Das Staatsministerium der Finanzen hat daraufhin an die nachgeordneten Behörden seines Geschäftsbereichs die folgenden Grundsätze zum Persönlichkeitsschutz bei Beihilfedaten erlassen, denen der ursprüngliche Entwurf der gemeinsamen Bekanntmachung zugrundeliegt (zit. n. Sen. Drucksache 37/85):

„1. Beihilfen werden nur auf Antrag unter Vorlage der entsprechenden Belege gewährt. Gemäß Nr. 14 Abs. 2 Satz 4 der Beihilfevor schriften sind die Anträge vertraulich zu behandeln. Die Bediensteten sollen die Beihilfeanträge und Belege (Art der Rechnungen, Rezepte, ärztliche Gutachten u. dgl.) in einem verschlossenen Umschlag einreichen. Diese Umschläge sind mit der Aufschrift „Beihilfe" zu kennzeichnen und dürfen nur von den Beihilfestellen geöffnet werden. Die Beschäftigungsdienststellen sind nicht berechtigt, die Weiterleitung der Beihilfeanträge von der offenen Vorlage der Antragsformulare und Belege abhängig zu machen.

2. Das allgemeine Persönlichkeitsrecht und seine Konkretisierung im sog. Recht auf „informationelle Selbstbestimmung" gebieten es, daß sämtliche Beihilfedaten grundsätzlich nur den mit der Beihilfesachbearbeitung befaßten Stellen zugänglich bleiben. Zu diesem Zweck ist eine strikte organisatorische und personelle Trennung von Beihilfe- und Personalsachbearbeitung, wie schon bisher auf Referentenebene, durchzuführen. Die Beihilfeakten sind getrennt von den Personalakten zu führen und aufzubewahren. Anläßlich von Versetzungen sind Personalakten und Beihilfeakten gesondert zu übersenden.

3. Das allgemeine Persönlichkeitsrecht und seine Konkretisierung im sog. Recht auf „informationelle Selbstbestimmung" erfordern auch ein generelles Verbot, Beihilfedaten zu anderen als Beihilfezwecken zu verwerten. Insbesondere dürfen die Beihilfe daten von Bediensteten grundsätzlich nicht für anderweitige dienstrechtliche Entscheidungen verwendet werden oder diese beeinflussen.

4. Weder das allgemeine Persönlichkeitsrecht noch das Recht auf „informationelle Selbstbestimmung" sind jedoch schrankenlos gewährleistet, vielmehr müssen Einschränkungen im überwiegenden Allgemeininteresse hingenommen werden. Bedienstete des Staates nehmen öffentliche, insbesondere hoheitliche Aufgaben wahr und stehen daher sowohl in einer erhöhten Pflichtenbindung gegenüber dem Dienstherrn als auch in einer gesteigerten Verantwort lichkeit gegenüber dem Bürger und der Öffentlichkeit. Hieraus folgt die Verpflichtung des Staates, im Rahmen des Möglichen zu verhindern, daß Bürger durch Bedienstete gefährdet werden oder zu Schaden kommen. Die Beihilfestellen sind daher bei einer erheblichen Gefährdung höherrangiger Gemeinschafts- oder Individualgüter berechtigt und im Einzelfall auch gehalten, dem Dienstvorgesetzten Mitteilung von derartigen Krankheiten ihrer Bediensteten zu machen. Dagegen berechtigen rein fiskalische Gründe – z.B. anläßlich von Lebenszeitverbeamtungen – die Beihilfestellen außer in den gesetzlich vorgeschriebenen Fällen keinesfalls zu entsprechenden Mitteilungen."

Die übrigen Staatsministerien haben, soweit erkennbar, für ihren Geschäftsbereich entsprechende Vorschriften erlassen. Das Staatsministerium des Innern beabsichtigte, den Gemeinden, Landkreisen, Bezirken und sonstigen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts zu empfehlen, entsprechend diesen Grundsätzen zu verfahren.

Ich begrüße ausdrücklich, daß die Staatsministerien nun Grundsätze zum Persönlichkeitsschutz bei Beihilfedaten erlassen haben. Sie stellen einen erheblichen Fortschritt dar. Gleichwohl habe ich dem Staatsministerium der Finanzen, den übrigen Gechäftsbereichen und dem Normprüfungsausschuß meine nach Erlaß der vorgenannten Grundsätze verbliebenen Bedenken mitgeteilt. Sie betreffen die beiden folgenden Punkte:

- Bei der organisatorischen Trennung von Beihilfsachbearbeitung und Personalverwaltung sind viele Behörden derzeit bereits weit über eine Trennung lediglich auf Sachbearbeiterebene (siehe Grundsätze, Nr. 2) hinausgegangen. Der Erlaß der Grundsätze zum Persönlichkeitsschutz bei Beihilfedaten sollte deshalb keinesfalls dazu führen solche weitergehenden organisatorischen Trennungen abzuschwächen oder gar rückgängig zu machen. Ich habe deshalb gebeten für die Zukunft zu prüfen, ob – außer bei obersten Dienstbehörden, in denen dies nicht durchführbar erscheint – eine Auslagerung der gesamten Beihilfeabrechnung aus der jeweiligen Behörde vorgesehen werden könnte. Kaum eine andere Abschottungsmaßnahme innerhalb einer Behörde selbst wird aus der Sicht der Beihilfeantragsteller einen gleichwertigen Schutz der Vertraulichkeit bewirken. Auf den Gedanken der Ausgliederung hatte ich bereits in einer Besprechung der Personalreferenten zum Thema Beihilfeorganisation hingewiesen.

- Der zweite Punkt, in dem keine volle Übereinstimmung der Ansichten erreicht wurde, sind die Ausnahmen von dem grundsätzlichen Verbot, Beihilfedaten für andere Zwecke als die Beihilfeabrechnung zu nutzen (siehe Grundsätze, Nr. 4). Angesichts der Gründe die gegen eine Nutzung von Beihilfedaten durch den Dienstherrn sprechen, die ich in meinem 6. Tätigkeitsbericht näher ausgeführt habe, hätte ich eine deutlich einschränkendere Ausnahmeregelung für geboten erachtet. So wäre m.E. infragegekommen, die Nutzungsberechtigung auch davon abhängig zu machen, daß keine anderen Erkenntnisquellen bestehen und daß außergewöhnliche Ausnahmesituationen vorliegen, sowie daß nach Abwägung aller Umstände des Einzelfalles wegen des Ausmaßes der Gefährdung der Schutz der Persönlichkeit zurücktreten muß. Ein Vorschlag, solche Einschränkungen einzuführen, lag dem Normprüfungsausschuß vor, wurde jedoch nicht aufgegriffen.

Darüber hinaus meine ich, daß auch rechtliche Zweifel an der Zulässigkeit der Ausnahmeregelung bestehen: Nach der neueren Rechtsprechung reicht zur Rechtfertigung von Grundrechtseinschränkungen – wie hier des Rechts auf informationelle Selbstbestimmung – das Institut des sogenannten besonderen Gewaltverhältnisses nicht aus. Vielmehr bedarf es eines Gesetzes, bzw. einer Sonderregelung im Grundgesetz selber.

Das Staatsministerium der Finanzen sieht nun eine derartige Sonderregelung im Grundgesetz selbst in Art. 33 Abs. 4 und 5 GG, wonach das Recht des öffentlichen Dienstes unter Berücksichtigung der hergebrachten Grundsätze des Berufsbeamtentums zu regeln ist. Zu diesen hergebrachten Grundsätzen des Berufsbeamtentums gehöre die Ausgestaltung des Beamtenverhältnisses als öffentlich rechtliches Dienst- und Treueverhältnisses. Die Grundrechte einerseits und das öffentlich rechtliche Dienst- und Treueverhältnis andererseits müßten im Wege der „praktischen Konkordanz" einander zugeordnet werden. Weder dürften die Grundrechte dem öffentlich rechtlichen Dienst- und Treueverhältnis geopfert werden, noch dürften die grundrechtlichen Gewährleistungen die Funktion des Beamtenverhältnisses unmöglich machen. Das Ausmaß der Grundrechtsschranken sei im Einzelfall im Hinblick auf Aufgabenbereich und Dienststellung des Beamten unter Beachtung des Grundsatzes der Verhältnismäßigkeit zu bestimmen.

Diese Auffassung stelle ich nicht infrage. Ich halte jedoch für fraglich, ob die vom Staatsministerium der Finanzen als Rechtsgrundlage für die Grundrechtseinschränkung herangezogenen Bestimmungen des Art. 33 Abs. 4 und 5 GG in Verbindung mit Ziffer 4 des Ministerialrundschreibens eine hinreichend normative Einschränkung des informationellen Selbstbestimmungsrechts des Beamten als Behilfeantragsteller darstellen (s.a. Maunz-Dürig-Herzog GG, RN 72 u. 83 zu Art. 33 GG: Gesetzesvorbehalt). Für die Familienangehörigen der Beamten (für die er Beihilfe-Anträge stellt) gelten diese Zweifel erst recht.

Nachdem in den Verhandlungen diese Frage offengeblieben war, begrüße ich es besonders, daß die neuen Beihilfevorschriften vom 19.4.1985 (FMBl S. 286 ff) nunmehr eine eindeutige datenschutzfreundliche Regelung enthalten:

„§ 17

....

(4) Die Beihilfeanträge sind unter Beifügung der Belege im Regelfall über die Beschäftigungsdienststelle der Festsetzungsstelle vorzulegen. Die bei der Bearbeitung der Beihilfen bekanntgewordenen Angelegenheiten sind geheimzuhalten. Sie dürfen nur für den Zweck verwandt werden, für den sie bekanntgegeben sind, es sei denn, es besteht eine gesetzliche Berechtigung oder Verpflichtung zur Offenbarung oder der Beihilfeberechtigte oder der Angehörige ist damit schriftlich einverstanden."

11.2. Zuordnung des betriebsärztlichen Dienstes einer Stadt zum Personalamt?

Durch einen Hinweis erfuhr ich, daß der betriebsärztliche Dienst einer Stadt dem Personalamt der Stadt organisatorisch zugeordnet wurde. Bisher war diese Einrichtung dem städtischen Gesundheitsamt angegliedert. Ich habe die Stadt auf Bedenken hingewiesen, die diese Neuorganisation unter Datenschutzgesichtspunkten auslöst: Die Tatsache eines Arztbesuches – auch beim Betriebsarzt – unterliegt der ärztlichen Schweigepflicht. Die organisatorische Zuordnung zum Personalamt könnte die gebotene Sicherstellung der diesbezüglichen Schweigepflicht infrage stellen. Im einzelnen: Nach § 3 Abs. 2 des Arbeitssicherungsgesetzes (ASiG) haben die Betriebsärzte u.a. die Aufgabe, die Arbeitnehmer zu untersuchen, arbeitsmedizinisch zu beurteilen und zu beraten sowie die Untersuchungsergebnisse zu erfassen und auszuwerten. Es ist daher wohl nicht auszuschließen, daß die organisatorische Zuordnung des betriebsärztlichen Dienstes zum Personalamt eine besondere Konfliktlage entstehen läßt, die aus den unterschiedlichen Aufgabenstellungen des Personalamts bzw. des betriebsärztlichen Dienstes resultiert.

Die ärztlich erhobenen Daten unterliegen einer strikten Zweckbindung: Nach § 8 Abs. 1 ASiG sind die Betriebsärzte bei der Anwendung ihrer Fachkunde weisungsfrei und nur ihrem ärztlichen Gewissen unterworfen. Sie haben die Regeln der ärztlichen Schweigepflicht zu beachten. Das gleichwohl bestehende datenschutzrechtlich bedeutsame Spannungsverhältnis wird dadurch etwas begrenzt, daß die Betriebsärzte unmittelbar dem Leiter des Betriebes unterstellt sind (§ 8 Abs. 2 ASiG) und ein unmittelbares Vorschlagsrecht beim zuständigen Mitglied des zur gesetzlichen Vertretung des Arbeitgebers berufenen Organs vorgesehen ist (§ 8 Abs. 3 ASiG).

Das Bundesverfassungsgericht hat im Volkszählungsurteil ausgeführt, daß entsprechend den bestehenden Gefährdungen mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen sind, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. Im Lichte dieser Ausführungen halte ich die Zuordnung des betriebsärztlichen Dienstes zum Personalamt nicht für eine Verstärkung organisatorischer und verfahrensrechtlicher Vorsorge gegen evtl. Verletzungen des Persönlichkeitsrechts im Zusammenhang mit Daten, die der Schweigepflicht unterliegen, sondern tendenziell eher für eine Abschwächung dieser Vorsorge. Außenstehenden bzw. den betroffenen Arbeitnehmern gegenüber könnte der Eindruck entstehen, daß die gesetzlich vorgesehene Weisungsfreiheit der Betriebsärzte durch die organisatorische Ansiedlung beim Personalamt tendenziell infrage gestellt sein könnte. Dies gilt um so mehr dann, wenn eine gemeinsame räumliche Unterbringung des Personalamts und des betriebsärztlichen Dienstes vorgesehen wäre, da die Kenntnisnahme des Arztbesuches durch das Personalamt ermöglicht wird. Ein solcher Eindruck sollte meines Erachtens bei der Entscheidung über die organisatorische Anbindung des betriebsärztlichen Dienstes vermieden werden, um das ungestörte Vertrauensverhältnis zwischen Betriebsarzt und Beschäftigten hinsichtlich des Umgangs mit personenbezogenen und sensiblen Daten als Voraussetzung für eine sinnvolle Tätigkeit des Betriebsarztes aufrecht zu erhalten.

Die Stadt hat mir mitgeteilt, daß eine räumliche Trennung des Personalamts vom betriebsärztlichen Dienst vorgesehen sei. Dadurch wurde die oben geschilderte datenschutzrechtliche Problematik zum Teil entschärft. Dennoch bleiben grundsätzliche Bedenken, die aus der unterschiedlichen Aufgabenstellung des Personalamts bzw. des betriebsärztlichen Dienstes resultieren.

11.3. Telefongesprächsdatenerfassung

Mit Fragen der Telefongesprächsdatenerfassung zu Abrechnungszwecken bin ich seit längerer Zeit befaßt. Bereits in meinem 3. Tätigkeitsbericht habe ich hierzu unter Ziffer 3.7.1 in dem Sinne Stellung genommen, daß ich die Registrierung dienstlicher Telefongespräche zu Abrech-

nungszwecken für zulässig erachte, gegen die umfassende Registrierung privater Telefongespräche von Bediensteten aber Bedenken habe.

1. Ich habe die Probleme der Telefondatenerfassung von Privatgesprächen der Bediensteten bei Behörden der Bayerischen Staatsverwaltung mit dem Bayerischen Staatsministerium des Innern und dem Bayerischen Staatsministerium der Finanzen in den vergangenen Monaten erörtert. Als Ergebnis dieser Erörterung kann festgestellt werden, daß der herrschenden Meinung zur Telefondatenerfassung von Privatgesprächen der Bediensteten insoweit gefolgt werden kann, als diese davon ausgeht, daß zwischen den beteiligten Gesprächspartnern kein Fernsprechgeheimnis besteht (vgl. Urteil des BVerwG vom 12.10.1983). Bei der Frage der Zulässigkeit der Speicherung und Nutzung der Daten eines privaten Telefonvorgangs unter Benutzung des Diensttelefons von Bedienste ten ist daher hinsichtlich des durch Art. 10 Grundgesetz geschützten Fernsprechgeheimnisses nicht die Einwilligung des angerufenen Dritten ausschlaggebend.

   Gleichwohl sind die Daten eines solchen Telefonvorgangs nicht schutzlos. Nach der Rechtsprechung des Bundesverfassungsgerichts zum Volkszählungsgesetz gibt es grundsätzlich kein belangloses Datum. Die Tatsache, daß ein Behördenbediensteter privat mit einem bestimmten Dritten telefoniert, der aufgrund der Speicherung der Zielnummer durch den Dienstherrn möglicherweise identifizierbar ist, kann einen sensiblen Bereich berühren. Den Anforderungen aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz, insbesondere des vom Bundesverfassungsgericht anerkannten informationellen Selbstbestimmungsrechts ist deshalb bei der Speicherung und Nutzung der Telefondaten von Privatgesprächen Rechnung zu tragen.

   Speicherung und Nutzung von Telefondaten bei Privatgesprächen sind daher aus der Sicht des Datenschutzes nur dann zulässig, wenn die Bediensteten darüber informiert sind, unter welchen Voraussetzungen sie den Dienstapparat für private Telefongespräche benutzen können. Der Dienstherr hat insbesondere darauf hinzuweisen, welche Daten im einzelnen gespeichert werden und welcher Nutzung sie zugeführt werden. Der Gewährleistung des Rechts auf informationelle Selbstbestimmung wäre es darüber hinaus dienlich, wenn den Bediensteten öffentliche Telefone in ausreichender Zahl und zumutbarer Entfernung zu Verfügung stünden, ggf. im Dienstgebäude.

   Unter diesen Voraussetzungen wird aus der Sicht des Datenschutzes zum Zwecke der Abrechnung der Kosten eine **Speicherung** der Daten eines privaten Telefonvorgangs einschließlich der angerufenen Zielnummer für zulässig erachtet. Allerdings ist im Hinblick auf den Schutz des Persönlichkeitsrechts bei der **Nutzung** dieser Daten dem Verhältnismäßigkeitsgrundsatz in besonderer Weise Rechnung zu tragen. Ein genereller Ausdruck von Uhrzeit, Dauer und angerufener Telefonnummer des Einzelgesprächs erscheint aus der Sicht des Datenschutzes in diesen Fällen nicht erforderlich. Im übrigen würde ein genereller Ausdruck dieser Daten nach Auffassung des Bayerischen Staatsministeriums der Finanzen eine entsprechende Unterrichtung der einzelnen Bediensteten und deren Zustimmung voraussetzen.

   Bei Abrechnungsschwierigkeiten, die auf Zweifeln eines betroffenen Bediensteten an der Verursachung der Höhe der Gebühreneinheiten beruhen, bestehen keine grundsätzlichen Bedenken gegen einen Ausdruck von Uhrzeit, Dauer und angerufener Zielnummer des strittigen **einzelnen** Telefongesprächs – ausschließlich zu Abrechnungszwecken. Gegen den Ausdruck **aller** zu einer Nebenstelle gespeicherten Daten auf Antrag des bzw. eines Benutzers der Nebenstelle unabhängig vom Bestehen von Abrechnungsschwierigkeiten bestehen aus der Sicht des Datenschutzes dann keine grundsätzlichen Bedenken, wenn und soweit durch Datensicherungsmaßnahmen sichergestellt ist, daß dadurch schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden; insbesondere muß durch solche Maßnahmen ausgeschlossen werden, daß andere Personen als die Betroffenen selbst vom Inhalt des Ausdrucks Kenntnis nehmen oder diesen anderweitig nutzen können.

   Der Zeitraum, in dem private Telefongespräche von Bediensteten registriert werden, sollte möglichst kurz sein, d.h. drei Monate nicht überschreiten, um das Anwachsen eines für andere Zwecke interessanten Auswertungspotentials möglichst zu vermeiden. Gegen eine weitere Speicherung der während der Abrechnungsperiode registrierten Daten für die Abwicklung der Bezahlung bis zu einem Zeitraum von 8 Wochen nach Ende der Abrechnungsperiode bestehen aus datenschutzrechtlicher Sicht keine Bedenken. Bestehen nach dieser 8-Wochen-Frist noch offene Abrechnungsfälle, sollten (nur) diese ausgedruckt und aktenmäßig weiterbehandelt werden. Der gesamte Datenträger müßte dann gesperrt werden. Da eine weitere Nutzung der gesperrten Daten nach diesem Zeitpunkt aber nicht mehr für zulässig gehalten wird, wird eine Löschung nach Ablauf der 8-Wochen- Frist für angemessen gehalten.

   Auch die aktenmäßig weiter zu behandelnden offenen Abrechnungsfälle sollten nach ihrer Aufklärung vernichtet werden.

   Während der Zeit der Speicherung ist für ausreichende Datensicherungsmaßnahmen zu sorgen. Kommt es unter den oben genannten Voraussetzungen zu einem Ausdruck der Einzeldaten, so müßte die Zuleitung an den Betroffenen in einem verschlossenen Umschlag erfolgen. Soweit Telefonregistrieranlagen es gestatten, die angerufene Telefonnummer verkürzt auszudrucken, hält es der Landesbeauftragte für den Datenschutz für geboten, hiervon Gebrauch zu machen. In Fällen, in denen die angefallenen Gespräche an Hand der angerufenen Nummer zugeordnet werden müssen, wäre dies beispielsweise in Betracht zu ziehen.

   Nach diesen Grundsätzen – soweit übertragbar – sollte auch bei manueller Aufzeichnung von Telefondaten von Privatgesprächen der Bediensteten verfahren werden.

2. Gegen die Registrierung dienstlicher Telefongespräche zu Abrechnungszwecken bestehen keine grundsätzlichen Bedenken aus der Sicht des Datenschutzes, da die öffentlichen Bediensteten insoweit als Amtswalter handeln, die ihrem Dienstherrn über die Art und Weise ihrer Amtsführung Rechenschaft schulden.

   Dieser Grundsatz für den dienstlichen Bereich kann aber meines Erachtens für Telefongespräche von Mitgliedern des Personalrates nicht zur Anwendung kommen.

Die Mitglieder des Personalrats stehen, soweit sie Aufgaben oder Befugnisse nach dem Bayerischen Personalvertretungsgesetz wahrnehmen, zwar in einem öffentlich-rechtlichen Dienstverhältnis, doch kommen den obersten Dienstbehörden und Dienststellenleitern insoweit nicht uneingeschränkte Dienstherrenrechte zu. Die Stellung der Mitglieder des Personalrats ist vielmehr geprägt von ihrem Mandat. Art. 8 Bayerisches Personalvertretungsgesetz bestimmt hierzu, daß Personen, die Aufgaben oder Befugnisse nach diesem Gesetz wahrnehmen, nicht darin behindert oder wegen ihrer Tätigkeit benachteiligt oder begünstigt werden dürfen.

In einem vergleichbaren Fall, in dem es um die Telefondatenerfassung der ehrenamtlichen Gemeinderäte ging, habe ich ausgeführt, daß die von den einzelnen Fraktionsmitgliedern als Mandatsträger geführten Telefongespräche keine Dienstgespräche in dem oben dargelegten Sinn seien. Solche Gespräche sollten als „Mandatsgespräche" bezeichnet werden. Die freie Ausübung des kommunalen Mandats umfaßt meines Erachtens auch das Recht Rathauspolitik ohne Kontrolle durch die Verwaltung vorzubereiten. Art. 30 Abs. 3 BayGO weist dem Gemeinderat als Kollegialorgan eine Überwachungsbefugnis gegenüber der Verwaltung zu. Die Zulassung der Telefongesprächserfassung der „Mandatsgespräche" würde zu einer Umkehrung dieser Kontrollbefugnis führen und den Schutz der freien Mandatsausübung ins Leere laufen lassen. Ein Kenntnisnahmerecht der Verwaltung und des 1. Bürgermeisters als Teil des Organs Gemeinderat besteht daher meines Erachtens nicht.

Diese Grundsätze müssen, wie ich glaube, entsprechend für die Mitglieder des Personalrates aufgrund ihrer Aufgaben und ihrer Stellung nach dem Bayer. Personalvertretungsrecht gelten. Die Aufzeichnung von Telefongesprächen der Mitglieder des Personalrats in ihrer Eigenschaft als Personalratsmitglieder ist nach meiner Auffassung geeignet, diese in ihren schutzwürdigen Belangen (Art. 1 und Art. 6 BayDSG) zu beeinträchtigen. Das Bayerische Staatsministerium der Finanzen hat mir allerdings mitgeteilt, daß nach dortiger Auffassung die Aufzeichnung von Telefondaten der Mitglieder des Personalrates in ihrer Eigenschaft als Personalratsmitglieder uneingeschränkt zulässig sei.

Um eine angemessene Behandlung dieser „Mandatsgespräche" zu gewährleisten, ließe sich für diese eine der sogenannten „Prominentenschaltung" entsprechende Schaltung einrichten. Darunter ist ein Nebenstellenanschluß zu verstehen, über den durch den installierten Telefoncomputer keinerlei Gesprächsdaten erfaßt werden. Im Vergleich zu den übrigen angeschlossenen Nebenstellen kommt er einem eigenständigen Telefonanschluß gleich. Eine Gebührenkontrolle ist allerdings bei einer Prominetenschaltung nicht möglich. Dabei verkenne ich nicht, daß auch die Mitglieder des Personalrates und des Gemeinderates an die Grundsätze der Wirtschaftlichkeit und Sparsamkeit gebunden sind.

Sollte daher aus haushaltsrechtlichen Gründen die Feststellung der durch die Mitglieder des Personalrates bzw. des Gemeinderates verursachten Telefongebühren erforderlich sein, so dürfte diese meines Erachtens nur aufgrund einer globalen Kontrolle getroffen werden, die keine Rückschlüsse auf das einzelne Mitglied oder einzelne Gespräch zuließe.

11.4. Darf die Personalstelle der Gemeinde Auskünfte über Mitarbeiter an deren Gläubiger oder an Kreditinstitute geben?

Anläßlich einer Besprechung über Datenschutz bei einer Gemeinde wurde von deren Personalstelle gefragt, welche Daten die Personalstelle über Gemeindebedienste an Gläubiger zum Zwecke der Einleitung einer Lohnpfändung offenbaren dürfe und ob Kreditinstituten Angaben über die Kreditwürdigkeit von Gemeindebediensteten gemacht werden dürften. Das von mir eingeschaltete Bayerische Staatsministerium des Innern hat hierzu die folgende sicherlich allgemein interessierende Auffassung vertreten:

Bei der Datenübermittlung an Gläubiger von Gemeindebediensteten zum Zwecke der Lohnpfändung ist zu unterscheiden:

- Wird der Gemeinde ein Pfändungsbeschluß des Vollstreckungsgerichts zugestellt (§ 829 ff ZPO), dann ist diese zur Übermittlung der in § 48 Abs. 1 ZPO genannten Daten berechtigt und verpflichtet.

- Die Zulässigkeit der Erteilung von Auskünften aufgrund sonstiger „einfacher" Anfragen von Gläubigern ist nach den Grundsätzen des Datenschutzrechts und des Personalaktenrechts zu beurteilen. Sofern entsprechende Daten aus einer Datei (Art. 5 Abs. 3 Nr. 3 BayDSG) übermittelt würden, ist dies nach Art. 18 Abs. 1 BayDSG nicht ohne Einwilligung des Betroffenen zulässig, da eine Beeinträchtigung dessen schutzwürdiger Belange sonst nicht ausgeschlossen werden könnte. Auch die prinzipielle Geheimhaltungspflicht für Personalakten (vgl. Art. 100 BayBG) steht der Erteilung einer derartigen Auskunft ohne Zustimmung des Betroffenen entgegen.

  Werden Daten nicht aus einer Datei übermittelt, kann die Regelung in Art. 18 BayDSG als allgemeiner Grundgedanke des Datenschutzrechts entsprechend herangezogen werden (vgl. auch Art. 30 Bayerisches Verwaltungsverfahrensgesetz, § 7 ADO). Eine Auskunft ist also auch in diesem Falle nicht ohne Unterrichtung und Zustimmung des Betroffenen zulässig.

Auch die Zulässigkeit einer Übermittlung von Angaben über die Kreditwürdigkeit von Gemeindebediensteten gegenüber Kreditinstituten ist nach Art. 18 Abs. 1 BayDSG bzw. in entsprechender Anwendung dieser Vorschrift und nach den Grundsätzen des Personalaktenrechts zu beurteilen. Da eine Beeinträchtigung schutzwürdiger Belange des Betroffenen bei einer Datenübermittlung nicht auszuschließen ist, können Angaben über Kreditwürdigkeit nur mit Zustimmung des Betroffenen gemacht werden.

11.5. Mitteilung über nicht rechtswidrige Sterilisation oder nicht rechtswidrigen Abbruch der Schwangerschaft bei Arbeitsunfähigkeit von BAT-Angestellten

Aufgrund einer Eingabe hatte ich das Formblatt „Mitteilung der Arbeitsunfähigkeit von BAT-Angestellten", Muster 7 EDVBA hinsichtlich des Datums „nicht rechtswidrige

Sterilisation, nicht rechtswidriger Abbruch der Schwangerschaft" datenschutzrechtlich zu überprüfen. Ich bin davon ausgegangen, daß die Dienstbehörde nur solche Angaben an die Staatsoberkasse übermitteln darf, die dort zur Aufgabenerfüllung erforderlich sind. Bei Übermittlung der Daten aus einer „Datei" folgt dies aus Art. 17 BayDSG. Auch wenn die Angabe nicht aus einer Datei entnommen wird, bestehen grundsätzlich keine Bedenken, den Rechtsgedanken des Erforderlichkeitsprinzips ebenfalls anzuwenden. Unter Berücksichtigung des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 halte ich es außerdem für geboten, bei Übermittlungen insbesondere sensibler Daten auch zu prüfen, ob sie gemessen an den Auswirkungen auf die Betroffenen als verhältnismäßig betrachtet werden können.

Zum Sachverhalt hat sich ergeben, daß die Daten „Krankheit", „Unfall" und „nicht rechtswidrige Sterilisation, nicht rechtswidriger Abbruch der Schwangerschaft" als Grund für die Arbeitsunfähigkeit so lange keine unterschiedlichen Rechtsfolgen nach sich ziehen, als die Dauer der Arbeitsunfähigkeit 6 Wochen nicht überschreitet (§ 47 Abs. 2 i.V.m. § 37 Abs. 1 und 2 BAT). Erst bei einer Arbeitsunfähigkeit über 6 Wochen hinaus werden die Krankenbezüge nur noch in den Fällen „Krankheit" oder „Unfall", nicht jedoch bei Sterilisation oder Schwangerschaftsabbruch bezahlt. In Fällen, in denen die Arbeitsunfähigkeit 6 Wochen überschreitet, ist im Hinblick auf die derzeitige Rechtslage nach § 37 Abs. 2 Satz 4 BAT die Erhebung und Mitteilung, wie sie in dem Formblattmuster 7 EDVBA vorgesehen ist, wohl erforderlich. In Fällen, in denen die Arbeitsunfähigkeit jedoch nicht länger als 6 Wochen besteht, ist eine Erhebung der Angabe „nicht rechtswidrige Sterilisation" oder „nicht rechtswidriger Abbruch der Schwangerschaft" dagegen nicht erforderlich, da dem Betroffenen für diese Zeit Krankenbezüge bezahlt werden ohne Unterschied, aus welchem Grund er arbeitsunfähig war. Ich habe deshalb angeregt, das Formblatt Muster 7 ADVBA so zu ändern, daß sichergestellt ist, daß Angaben zum Datum „nicht rechtswidrige Sterilisation, nicht rechtswidriger Abbruch der Schwangerschaft" nur dann zu machen sind, wenn die Zeit der Arbeitsunfähigkeit 6 Wochen überschreitet.

Darüber hinaus habe ich zu bedenken gegeben, daß die Erhebung und Übermittlung der Daten „nicht rechtswidrige Sterilisation, nicht rechtswidriger Abbruch einer Schwangerschaft" als Grund einer Arbeitsunfähigkeit, die länger als 6 Wochen besteht – wenn dies auch in der genannten Vorschrift des BAT so vorgesehen ist – unter dem Gesichtspunkt der Verhältnismäßigkeit zweifelhaft sein kann und ich habe angeregt zu überprüfen, ob der fiskalische Nutzen (Einsparung von Haushaltsmitteln) zur Intensität des Eingriffs, der in der Erhebung dieser Daten liegt, noch in einem angemessenen Verhältnis steht und damit die Erhebung und Nutzung dieser Angabe rechtfertigen kann. Es handelt sich um besonders sensible Angaben über den Betroffenen, die auf diese Weise dem Arbeitgeber bekannt würden. Dies steht im Gegensatz zu der sonstigen Praxis, die von dem Grundsatz ausgeht, daß der Arbeitgeber nur die Tatsache der Erkrankung bzw. des Unfalls erfährt, nicht aber den Grund bzw. die ärztliche Diagnose.

Nunmehr wurde das Muster 7 EDVBA so abgeändert, daß Angaben über nicht rechtswidrige Sterilisation bzw. nicht rechtswidrigen Abbruch der Schwangerschaft bei Arbeitsunfähigkeiten unter 6 Wochen nicht zu erheben sind.

11.6. Weitergabe von Anschriften von Bewerbern für die Beamtenlaufbahn an Versicherungen

Im Berichtszeitraum häuften sich erneut die Eingaben von jungen Beamten, die sich durch eine offenbar gezielte Weitergabe ihrer Anschriften an verschiedene, teils öffentlich-rechtliche, teils private Versicherungen in ihren schutzwürdigen Belangen und in ihrer Privatsphäre verletzt fühlten. Bei einigen dieser Beamten haben die Versicherungsvertreter sogar schon vorgesprochen, bevor dem Bewerber die Einstellungszusage bekannt gegeben worden war.

Aufgrund dieses Umstandes habe ich alle obersten Dienstbehörden des Freistaates (Staatskanzlei und Ministerien) gebeten, darauf zu achten, daß insbesondere Mitarbeiter der eigenen Personalverwaltungen und der der nachgeordneten Dienststellen keine Nebentätigkeiten ausüben, die zu einer Interessenkollision Dienstherr/Versicherung führen könnten. In den Antworten der Geschäftsbereiche wurde mir zugesichert, diese Möglichkeit einer unzulässigen Datenweitergabe durch geeignete Maßnahmen zumindest weitestgehend einzuschränken.

Die Auffassung mancher Versicherung, die Fürsorgepflicht des Dienstherrn gebiete es, seine Beamten auf mögliche Versorgungslücken während des Vorbereitungsdienstes hinzuweisen und dabei auch die Beamtenversicherungen als Selbsthilfeeinrichtungen hervorzuheben, vermag eine Datenweitergabe ohne vorherige Zustimmung der Betroffenen nicht zu rechtfertigen.

11.7. Personalsachbearbeiter oder Ausbildungsleiter als Vertrauensmann für eine Versicherung?

Aufgrund verschiedener Hinweise hatte ich mich mit der Frage zu befassen, ob aus der Sicht des Datenschutzes Bedenken gegen eine Tätigkeit von Personalsachbearbeitern oder Ausbildungsleitern als Vertrauensmann für eine Versicherung bestehen. Unabhängig von Fragen des Nebentätigkeitsrechts, die sich hier primär stellen, für deren Klärung ich jedoch nicht zuständig bin, habe ich dazu die folgende Ansicht vertreten:

Werden Bedienstete, die mit personenbezogenen Daten aus der Personalverwaltung oder dem Ausbildungsbereich zu tun haben, gleichzeitig beim Abschluß von Versicherungsverträgen – insbesondere Krankenversicherungsverträgen – tätig, so können sich hier die folgenden Probleme ergeben: Die Bediensteten könnten u.U. Kenntnisse aus dem Personal- oder Ausbildungsbereich (also „Daten" aus diesem Bereich) für andere Zwecke, nämlich die Werbung und den Abschluß von Versicherungsverträgen (z.B. bei Beamten-Selbsthilfeeinrichtungen) verwerten. Umgekehrt könnten Kenntnisse aus der Beratung und dem Abschluß für Versicherungen bewußt oder unbewußt im Personalverwaltungs- oder Ausbildungsbereich Verwendung finden. In der Terminologie des Datenschutzes handelt es sich um eine Änderung des Verwendungszwecks der personenbezogenen Daten, für die im jeweiligen Bereich „Personal" bzw. „Versicherung" an sich grundsätzlich Verschwiegenheitspflichten bzw. Vertrauensschutz gegenüber dem Betroffenen bestehen.

Unabhängig davon, ob die entsprechenden Angaben in einer Datei oder auf anderen Datenträgern festgehalten sind oder im Rahmen der Beratung bei Erhebung von Daten den Betreffenden bekannt werden, werden solche Angaben vom Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfaßt. Einschränkungen dieses Grundrechts, die auch in einer zweckwidrigen Verwendung von Daten liegen können, setzen eine rechtliche Befugnis voraus. Da entsprechende gesetzliche Befugnisse in diesem Fall fehlen, wäre im Einzelfall zu prüfen, ob konkludente Einwilligungen der Betroffenen angenommen werden könnten. Dabei halte ich für zweifelhaft, ob solche Einwilligungen stets unterstellt werden können. Im Falle von Anwärtern beispielsweise kann wegen der Gefahr der psychischen Beeinflussung der Betroffenen eine konkludente Einwilligung in die zweckentfremdete Nutzung der Daten aus dem jeweiligen Bereich nicht angenommen werden. Es ist wohl davon auszugehen, daß sich hier in vielen Fällen die Betroffenen unfreiwillig der gegebenen Situation einer möglichen Vermischung bei der Nutzung von Daten aus dem Personal- an den Versicherungsbereich beugen. Für problematisch wäre auch der Fall zu betrachten, daß bei der Erweiterung von Krankenversicherungsverträgen oder bei der Erörterung von Krankheiten, die zu Wartezeiten oder Ausschlüssen bei der Versicherung führen, Kenntnis von genaueren Krankheitsumständen des Betroffenen oder seiner Angehörigen erlangt wird. Anders mag es sich im Einzelfall bei der Tätigkeit von Vertrauensleuten handeln, wenn diese für Kollegen tätig werden, die bereits seit längerem verbeamtet sind, ohne daß dabei derartige zusätzliche Informationen über Krankheitsumstände offenbar werden.

Aus der Sicht des Datenschutzes bestehen daher erhebliche Bedenken hinsichtlich der Vereinbarkeit der Tätigkeit als Vertrauensmann für eine Versicherung (insbesondere Krankenversicherung) und einer Tätigkeit, bei der dem Betreffenden personenbezogene Angaben der Bediensteten aus dem Personal- oder Ausbildungsbereich bekannt sind. Die Bedenken gelten auch gegenüber der entsprechenden Regelung des Nebentätigkeitsrechts.

11.8. Weitergabe von Personaldaten zur Veröffentlichung durch Verbände

Auf die Darstellung des Problems im 6. Tätigkeitsbericht unter Nr. 4.9.8 (Seite 60/61) wird verwiesen. Das Bayerische Staatsministerium der Finanzen, das in Personalangelegenheiten federführend ist, hat mir mitgeteilt, daß es meine Auffassung bezüglich der Rechtslage bei der Weitergabe von Personaldaten an Berufsverbände zur Veröffentlichung in Verbandsorganen im Grundsatz teile. Die Bayerische Finanzverwaltung werde deshalb personenbezogene Daten nur noch weitergeben, wenn die Einwilligung der betroffenen Bediensteten vorliege. Dabei werde bei Mitgliedern der Verbände der Nachweis der Unterwerfung unter eine entsprechende Satzungsbestimmung als hinreichend erachtet; bei Nichtmitgliedern werde der Nachweis einer schriftlichen Zustimmung im Einzelfall gefordert werden.

12. Statistik

12.1. Mikrozensus 1985

Die Datenschutzbeauftragten des Bundes und der Länder befaßten sich im Berichtsjahr mit Entwürfen zum Mikrozensusgesetz. Inzwischen ist der Mikrozensus 1985 im Gange.

Im Vergleich zu der vom Bundesverfassungsgericht seinerzeit ausgesetzten Volkszählung 1983 erscheint die Mikrozensuserhebung – gemessen an den Kriterien des Volkszählungsurteils – weniger gravierend. Hinsichtlich der Sensibilität der erhobenen Daten hat sich an dem früheren Urteil des Bundesverfassungsgerichts über die Verfassungsmäßigkeit des Mikrozensus nichts wesentliches geändert – insbesondere, da die erhobenen Daten nicht zu anderen Zwecken als Statistiken der Stat. Landesämter verwendet werden. Eine Weitergabe von Einzeldaten an andere Stellen zur weiteren Auswertung findet in diesem Fall überhaupt nicht statt, während eine solche im Volkszählungsgesetz 1983 zugelassen war. Auch die moderne automatisierte Datenverarbeitung hat die Rahmenbedingungen speziell für den Mikrozensus – im Gegensatz zur Volkszählung – nicht wesentlich verändert, da ausschließlich innerhalb der statistischen Ämter verarbeitet wird. Eine dem Volkszählungsverfahren vergleichbare Menge von Zählern wird nicht benötigt. In Bayern wird die Erhebung durch Kräfte vorgenommen, die dem Landesamt für Statistik und Datenverarbeitung überwiegend seit längerem als zuverlässig bekannt sind. Der ebenfalls ins Spiel gebrachte Gedanke einer freiwilligen Durchführung des Mikrozensus ist noch nicht so ausgereift, daß er als einwandfrei gelöstes Problem gelten könnte. Im Mikrozensusgesetz 1985 ist zudem eine Testerhebung mit freiwilliger Auskunftserteilung vorgesehen, um zu prüfen, ob in künftigen Mikrozensuserhebungen ganz oder teilweise auf die Auskunftspflicht verzichtet werden kann.

Bei Anfragen, die den Landesbeauftragten für den Datenschutz aus der Bevölkerung erreichten, konnten datenschutzrechtliche Bedenken in der Regel ausgeräumt werden.

12.2. Volkszählung

Bei Redaktionsschluß des vorliegenden Tätigkeitsberichts war ein neues Volkszählungsgesetz – etwa für ein Volkszählung 1986 – noch nicht erlassen. Die Bundesregierung hatte allerdings einen Entwurf für ein Volkszählungsgesetz 1986 eingebracht. Der Entwurf zieht in vielen Einzelpunkten Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts. So enthält er Bestimmungen über die Abschottung von Erhebungsstellen vom Vollzug anderer Aufgaben der Gemeinden, zur Interessenkollision von Zählern, zur Trennung von Erhebungsmerkmalen und Hilfsmerkmalen sowie zur Vernichtung der Erhebungsvordrucke und Löschung von Ordnungsnummern und schließlich zur Unterrichtung des Auskunftspflichtigen. Die Anschrift soll nur noch als Hilfsmerkmal erhoben werden und auf die Übermittlung von Einzelangaben an oberste Bundes- und Landesbehörden – ein vom Bundesverfassungsgericht beim letzten Volkszählungsgesetz kriti-

sierter Punkt – soll verzichtet werden. Meinungsverschiedenheiten bestanden, soweit bekannt, zur Frage wie weit den erhebenden Gemeinden in mehr oder weniger bescheidenem Maße eine Auswertung von Einzeldaten für eigene Statistikzwecke zugestanden werden soll. Endgültige Aussagen hierzu sind noch nicht möglich.

Ganz allgemein sei jedoch folgendes zum wiederholtem Male festgehalten: Statistiken, wie auch die Volkszählung, werden in einem vom sonstigen Verwaltungsvollzug getrennten Verfahren durchgeführt. Datenerhebung, Speicherung und Nutzung sind – von wenigen gesetzlich definierten Ausnahmefällen abgesehen – vom Vollzugs-Verwaltungsverfahren getrennt. Die Bemühungen des Gesetzgebers bei der Schaffung des neuen Volkszählungsgesetzes richten sich besonders auf diese Abtrennung. Auch wenn er dabei an einigen Punkten keine hundertprozentige Sicherung der Daten gegen Kenntnisnahme beispielsweise von Zählern oder von Beamten in Erhebungsstellen erreichen sollte, ist diesem selbständigen Statistikverfahren aus der Sicht der Betroffenen und damit des Datenschutzes bei weitem der Vorzug zu geben vor einer möglichen Alternative: Nämlich der Verfügbarmachung entsprechender personenbezogener Daten aus dem Verwaltungsvollzug. Wie schon mehrfach ausgeführt und auch vom Bundesverfassungsgericht im Volkszählungsurteil aufgegriffen, wäre die Herstellung einer Datenübermittlungs- und Verknüpfungsinfrastruktur, die die Gewinnung von Volkszählungsdaten aus dem Verwaltungsvollzug zum Ziele hätte, äußerst problematisch. Es würde mit den damit geschaffenen Datenübermittlungs- und Verknüpfungsmöglichkeiten nämlich die Zusammenführung von weit mehr Daten als nur derjenigen, die für Volkszählungszwecke gesammelt werden müßten, ermöglicht. Auch würden Datenflüsse vorbereitet, die bisher zwischen Behörden nicht bestehen. Es würde mit der Infrastruktur für solche Datenflüsse und Verknüpfungen der Boden für umfassendere Datensammlungen bereitet, als sie bisher bestehen. Sie wären für die Betroffenen keineswegs akzeptabler als eine mit den möglichen Sicherheitsvorkehrungen ausgestattete Volkszählung. Zu möglichen Folgen intensiver Sammlung von Daten hat das Bundesverfassungsgericht im Zusammenhang mit der Geheimhaltung von steuerlichen Angaben in der Entscheidung über Untersuchungsausschüsse des Bundestags folgendes ausgeführt:

„Die Angaben, die ein Steuerpflichtiger aufgrund des geltenden Abgabenrechts zu machen hat, ermöglichen weitreichende Einblicke in die persönlichen Verhältnisse, die persönliche Lebensführung (bis hin beispielsweise zu gesundheitlichen Gebrechen, religiösen Bindungen, Ehe- und Familienverhältnissen oder politischen Verbindungen) und in die beruflichen, betrieblichen, unternehmerischen oder sonstigen wirtschaftlichen Verhältnisse. Über ihre zeitlich kontinuierliche Erfassung, Speicherung und ständige Abrufbarkeit ermöglichen sie demjenigen, der über diese Daten verfügt, ein Wissen außerordentlichen Ausmaßes über die Betroffenen, das unter den gegenwärtigen Lebensverhältnissen in entsprechende Macht über die Betroffenen umschlagen kann." (BVerfGE 67,100 (142/43)).

Die Schaffung von neuen Datenübermittlungs- und Verknüpfungsinfrastrukturen als Ersatz für eine selbständige Statistik bzw. Volkszählung kann also keinesfalls als ein „kleineres Übel" im Verhältnis zu statistischen Erhebungen betrachtet werden.

12.3. Statistikdaten für Regionalplanung

Aufgrund der Anfrage einer Behörde hatte ich mich mit der Frage zu befassen, ob und inwieweit Regionalplanung unmittelbaren Verwaltungsvollzugscharakter besitzt. Dies ist von Bedeutung für die Frage, ob statistische Daten die auch nach der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 grundsätzlich nicht für Zwecke des Verwaltungsvollzugs verwendet werden dürfen, für Zwecke der Regionalplanung verwendet werden könnten, ohne mit diesem Verbot in Konflikt zu geraten. Ich habe hierzu folgende Ansicht vertreten:

Das Bundesverfassungsgericht hat in seinem Urteil die im § 9 Abs. 3 Satz 1 des Volkszählungsgesetzes 1983 vorgesehene Übermittlung von Einzelangaben ohne Namen für Zwecke der Regionalplanung für nichtig erklärt.

Regionalplanung, als Teil der Landesplanung ist überörtliche Planung. Sie trifft grundsätzlich keine Festsetzungen oder Verwaltungsentscheidungen gegenüber dem einzelnen Bürger (§ 3 Abs. 3 und § 5 Abs. 4 i.V.m. § 4 Abs. 5 ROG). Raumordnung und Landesplanung sind daher nicht dem unmittelbaren Verwaltungsvollzug zuzurechnen; ihre Aufgabe ist vielmehr die Aufstellung und Fortschreibung von übergeordneten und zusammenfassenden Programmen und Plänen sowie die Abstimmung raumbedeutsamer Maßnahmen und Planungen im Vorfeld des eigentlichen Verwaltungsvollzugs.

Die Ziele der Raumordnung und Landesplanung und damit auch der Regionalplanung sind regelmäßig Grundsätze der Entwicklung. Festlegungen für konkrete Einzelfälle können sich dabei nur ergeben, wenn es sich aus zwingenden landesplanerischen und raumordnerischen Belangen als erforderlich erweist – beispielsweise wenn für ein Objekt nur ein bestimmter Standort in Frage kommt. In diesen Ausnahme-Fällen kann und muß die Raumordnung und Landesplanung einschließlich der Regionalplanung über die gemeindliche Anpassungspflicht nach § 1 Abs. 4 Bundesbaugesetz dem einzelnen Bürger gegenüber konkrete Wirkungen entfalten. In diesen Ausnahmefällen wären Festlegungen von Zielen der Raumordnung und Landesplanung daher dem Verwaltungsvollzug zuzurechnen.

Im Hinblick darauf müßten bei Verwendung von Daten aus statistischen Erhebungen für die Regionalplanung Regelungen geschaffen werden, die den Erfordernissen des Urteils zum Volkszählungsgesetz entsprechen.

12.4. Hochschulstatistik

Siehe 13.5

12.5. Keine namentliche Befragung von Schülern mehr nach ihren Studien- und Berufswünschen

In meinem 3. Tätigkeitsbericht hatte ich auf Eingaben von Schülern hingewiesen, in denen Beschwerde darüber geführt worden war, daß die statistische Erhebung über die Studien- und Berufswünsche von Abiturienten mit der Bekanntgabe des Namens des Schülers verbunden wurde. Ich hatte dazu die Ansicht vertreten, daß die Erhebung des

Namens, die nach dem Hochschulstatistikgesetz nicht vorgeschrieben ist, unverhältnismäßig sei. Auch hatten nicht alle statistischen Ämter der Bundesrepublik die Namensangabe gefordert.

Mit Schreiben vom 2.1.1985 wurde ich nun vom Bayerischen Staatsministerium für Unterricht und Kultus darüber unterrichtet, daß die Statistik über die Studien- und Berufswünsche im Schuljahr 1984/85 erstmals ohne Erhebung der Namen der zu befragenden Schüler durchgeführt werde. Auch innerhalb des Schulbereichs erfolge die Erhebung anonym, d.h. auch die Schule kann nicht über irgendwelche Nummernverzeichnisse die ausgefüllten Fragebogen bestimmten Personen zuordnen.

13. Schule und Hochschule

Im Bereich der Schul- und Hochschulverwaltung haben mich Bürger zu den schon aus früheren Tätigkeitsberichten bekannten Problemen angesprochen: Datenerhebungen in der Schule für schulische Zwecke, der Inhalt von Jahresberichten, die Übermittlung von Schülerdaten an andere Schulen beim Schulwechsel sowie allgemein Datenerhebung und Datenübermittlung für Forschungszwecke unter Einschluß sehr privater Daten. Auf diese Fragen werde ich im folgenden kurz eingehen.

Im Hochschulbereich lag ein Schwerpunkt meiner Tätigkeit im Berichtszeitraum bei den Überlegungen zur Hochschulstatistik. Die bisher fehlende Trennung der Datenverarbeitung für die Hochschulverwaltung und die Hochschulstatistik erfordert nicht zuletzt im Hinblick auf das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 eine Novellierung der entsprechenden gesetzlichen Bestimmungen. Hier zeichnen sich meines Erachtens durchaus gangbare Wege ab.

13.1. Persönlichkeitsschutz an Schulen

Es ist eine alte Erfahrung, daß die Schule prägende Einflüsse bei den Kindern hinterläßt und somit entscheidend das künftige gesellschaftliche Verhalten der Kinder mitbestimmt. Dies gilt bis zu einem gewissen Grade auch für die Erfahrungen der Kinder mit dem allgemeinen Persönlichkeitsschutz und demzufolge mit dem Datenschutz. Werden Kinder im Rahmen der üblichen Unterrichtsgestaltung oder für Verwaltungszwecke öffentlich vor allen anderen Kinder immer wieder über private Lebensverhältnisse befragt, mag dies Auswirkungen auf die Einstellung zur Notwendigkeit der Achtung der Privatsphäre anderer haben. Zu diesem Thema gebe ich im folgenden einen Auszug aus dem 7. Tätigkeitsbericht des Schleswig-Holsteinischen Landesbeauftragten für den Datenschutz wieder. Ich meine, daß diese Passage recht nachdenklich stimmt:

> Aber auch Sorgen, die aus der Unterrichtsgestaltung herrühren, werden an den Landesbeauftragten herangetragen. Sie sind zwar nicht dem Datenschutz im engeren Sinne zuzurechnen, zeigen doch aber wenig diskreten Umgang mit personenbezogenen Daten. So heißt es in einer Beschwerde wörtlich:
>
> „Es gab ja früher in den Schulen Gewohnheiten, die alle Kinder aus kaputten Verhältnissen fürchteten. So die öffentlichen Abfragungen und Eintragungen in das Klassenbuch. Unsere Zeit hat reformiert und jenen Sadismus durch einen besseren ersetzt. Da nehmen die Kinder Stammbäume in der Schule durch. Hinterher schreiben sie eine Arbeit. Wenn die unehelichen Kinder keine Väter eintragen, bekommen sie schlechte Noten. Ein Kind ist in hemmungsloses Weinen ausgebrochen. Die Mutter hat mehrere Kinder von mehreren Vätern und wenn es zuhause fragt, bekommt es eines hinter die Ohren."
>
> An anderer Stelle ist zu lesen:
>
> „Nach dem Lehrplan für die Grundschule sollen die Kinder im Unterricht verschiedene Angaben über ihre Lebensverhältnisse machen. So schon im ersten Schuljahr über Beruf, Freizeitgestaltung und Auseinandersetzungen der Eltern, Stammbaum (mit Lichtbildern) und Krankheiten der Familie, Grundriß und Baumbestand des Elternhauses, Haustiere und Spielzeug des Kindes bzw. der Elten. Im Unterricht wurden entsprechende Fragen bereits bis ins Bett hinein vertieft. Mein Sohn wird in der Klasse entspechend unter Druck gesetzt, wenn er die Beantwortung ablehnen will. Die Lehrerin soll auch erfragte Daten notiert haben. ... In anderen Grundschulen soll es Fragen nach den reichsten Dorfbewohnern, nach der Parteizugehörigkeit der Eltern und nach dem Schrifttum des Elternhauses gegeben haben."
>
> Derartige Fragen dringen ohne Not tief in den intimen Bereich des privaten Lebens ein.

Auch an bayerischen Schulen gibt es gelegentlich Probleme mit der Erstellung von Stammbäumen.

So hat sich ein Vater an mich gewandt, dessen Tochter im vierten Grundschuljahr als Hausaufgabe das Erstellen eines Stammbaumes aufbekommen hatte. Zu diesem Zweck war dem Kind ein umfangreiches Formblatt ausgehändigt worden, in das es neben persönlichen Angaben zu sich selbst ein Foto einkleben sollte. Des weiteren waren Angaben zu den Eltern, den vier Großeltern und den acht Urgroßeltern in das Formblatt einzutragen. Anzugeben waren die Namen, die Hochzeitstage und die Sterbetage.

Der Vater hat mir hierzu folgendes mitgeteilt:

„Dieses Formblatt, allerdings in Verbindung mit der gestellten Hausaufgabe, rief nun gleichermaßen sowohl im Familienkreise als auch bei Freunden und Bekannten zumindest Erstaunen hervor und gleichfalls unselige Erinnerungen wach. Ältere erinnerten sich an gleiche Hausaufgaben in den Jahren 1933 – 1945."

Das Bayerische Staatsministerium für Unterricht und Kultus hat hierzu mitgeteilt, daß im Lehrplan für das Fach Heimat- und Sachkunde zwar das Lernziel „Einblick in das Leben der Familien früher und heute" enthalten sei, dabei sollten ins Detail gehende Stammbäume aber nicht erstellt werden. Das Aufzeigen der Ahnenreihe ist in einer Weise geschehen, die sowohl die Gefühle des einzelnen Schülers achtet als auch dem Anliegen des Datenschutzes Rechnung trägt. Das im vorliegenden Fall verwendete sehr detaillierte Formblatt

Namens, die nach dem Hochschulstatistikgesetz nicht vorgeschrieben ist, unverhältnismäßig sei. Auch hatten nicht alle statistischen Ämter der Bundesrepublik die Namensangabe gefordert.

Mit Schreiben vom 2.1.1985 wurde ich nun vom Bayerischen Staatsministerium für Unterricht und Kultus darüber unterrichtet, daß die Statistik über die Studien- und Berufswünsche im Schuljahr 1984/85 erstmals ohne Erhebung der Namen der zu befragenden Schüler durchgeführt werde. Auch innerhalb des Schulbereichs erfolge die Erhebung anonym, d.h. auch die Schule kann nicht über irgendwelche Nummernverzeichnisse die ausgefüllten Fragebogen bestimmten Personen zuordnen.

13. Schule und Hochschule

Im Bereich der Schul- und Hochschulverwaltung haben mich Bürger zu den schon aus früheren Tätigkeitsberichten bekannten Problemen angesprochen: Datenerhebungen in der Schule für schulische Zwecke, der Inhalt von Jahresberichten, die Übermittlung von Schülerdaten an andere Schulen beim Schulwechsel sowie allgemein Datenerhebung und Datenübermittlung für Forschungszwecke unter Einschluß sehr privater Daten. Auf diese Fragen werde ich im folgenden kurz eingehen.

Im Hochschulbereich lag ein Schwerpunkt meiner Tätigkeit im Berichtszeitraum bei den Überlegungen zur Hochschulstatistik. Die bisher fehlende Trennung der Datenverarbeitung für die Hochschulverwaltung und die Hochschulstatistik erfordert nicht zuletzt im Hinblick auf das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 eine Novellierung der entsprechenden gesetzlichen Bestimmungen. Hier zeichnen sich meines Erachtens durchaus gangbare Wege ab.

13.1. Persönlichkeitsschutz an Schulen

Es ist eine alte Erfahrung, daß die Schule prägende Einflüsse bei den Kindern hinterläßt und somit entscheidend das künftige gesellschaftliche Verhalten der Kinder mitbestimmt. Dies gilt bis zu einem gewissen Grade auch für die Erfahrungen der Kinder mit dem allgemeinen Persönlichkeitsschutz und demzufolge mit dem Datenschutz. Werden Kinder im Rahmen der üblichen Unterrichtsgestaltung oder für Verwaltungszwecke öffentlich vor allen anderen Kinder immer wieder über private Lebensverhältnisse befragt, mag dies Auswirkungen auf die Einstellung zur Notwendigkeit der Achtung der Privatsphäre anderer haben. Zu diesem Thema gebe ich im folgenden einen Auszug aus dem 7. Tätigkeitsbericht des Schleswig-Holsteinischen Landesbeauftragten für den Datenschutz wieder. Ich meine, daß diese Passage recht nachdenklich stimmt:

> Aber auch Sorgen, die aus der Unterrichtsgestaltung herrühren, werden an den Landesbeauftragten herangetragen. Sie sind zwar nicht dem Datenschutz im engeren Sinne zuzurechnen, zeigen doch aber wenig diskreten Umgang mit personenbezogenen Daten. So heißt es in einer Beschwerde wörtlich:
>
> „Es gab ja früher in den Schulen Gewohnheiten, die alle Kinder aus kaputten Verhältnissen fürchteten. So die öffentlichen Abfragungen und Eintragungen in das Klassenbuch. Unsere Zeit hat reformiert und jenen Sadismus durch einen besseren ersetzt. Da nehmen die Kinder Stammbäume in der Schule durch. Hinterher schreiben sie eine Arbeit. Wenn die unehelichen Kinder keine Väter eintragen, bekommen sie schlechte Noten. Ein Kind ist in hemmungsloses Weinen ausgebrochen. Die Mutter hat mehrere Kinder von mehreren Vätern und wenn es zuhause fragt, bekommt es eines hinter die Ohren."
>
> An anderer Stelle ist zu lesen:
>
> „Nach dem Lehrplan für die Grundschule sollen die Kinder im Unterricht verschiedene Angaben über ihre Lebensverhältnisse machen. So schon im ersten Schuljahr über Beruf, Freizeitgestaltung und Auseinandersetzungen der Eltern, Stammbaum (mit Lichtbildern) und Krankheiten der Familie, Grundriß und Baumbestand des Elternhauses, Haustiere und Spielzeug des Kindes bzw. der Elten. Im Unterricht wurden entsprechende Fragen bereits bis ins Bett hinein vertieft. Mein Sohn wird in der Klasse entspechend unter Druck gesetzt, wenn er die Beantwortung ablehnen will. Die Lehrerin soll auch erfragte Daten notiert haben. ... In anderen Grundschulen soll es Fragen nach den reichsten Dorfbewohnern, nach der Parteizugehörigkeit der Eltern und nach dem Schrifttum des Elternhauses gegeben haben."
>
> Derartige Fragen dringen ohne Not tief in den intimen Bereich des privaten Lebens ein.

Auch an bayerischen Schulen gibt es gelegentlich Probleme mit der Erstellung von Stammbäumen.

So hat sich ein Vater an mich gewandt, dessen Tochter im vierten Grundschuljahr als Hausaufgabe das Erstellen eines Stammbaumes aufbekommen hatte. Zu diesem Zweck war dem Kind ein umfangreiches Formblatt ausgehändigt worden, in das es neben persönlichen Angaben zu sich selbst ein Foto einkleben sollte. Des weiteren waren Angaben zu den Eltern, den vier Großeltern und den acht Urgroßeltern in das Formblatt einzutragen. Anzugeben waren die Namen, die Hochzeitstage und die Sterbetage.

Der Vater hat mir hierzu folgendes mitgeteilt:

„Dieses Formblatt, allerdings in Verbindung mit der gestellten Hausaufgabe, rief nun gleichermaßen sowohl im Familienkreise als auch bei Freunden und Bekannten zumindest Erstaunen hervor und gleichfalls unselige Erinnerungen wach. Ältere erinnerten sich an gleiche Hausaufgaben in den Jahren 1933 – 1945."

Das Bayerische Staatsministerium für Unterricht und Kultus hat hierzu mitgeteilt, daß im Lehrplan für das Fach Heimat- und Sachkunde zwar das Lernziel „Einblick in das Leben der Familien früher und heute" enthalten sei, dabei sollten ins Detail gehende Stammbäume aber nicht erstellt werden. Das Aufzeigen der Ahnenreihe ist in einer Weise geschehen, die sowohl die Gefühle des einzelnen Schülers achtet als auch dem Anliegen des Datenschutzes Rechnung trägt. Das im vorliegenden Fall verwendete sehr detaillierte Formblatt

ergeben hatten, daß im weiterführenden Schulsektor bis zu 110 Gastschülermeldungen unberücksichtigt geblieben seien, was allein zu einem Einnahmeausfall von ca. 110.000,- DM geführt habe, sei eine vollständigere Erfassung der Gastschüler geplant gewesen.

Das Befragungsblatt hat in der zunächst vorliegenden Fassung weder den Voraussetzungen des Art. 16 Abs. 2 BayDSG noch des Art. 62 Abs. 1 Satz 3 BayEUG entsprochen. Hiernach ist gesetzlich vorgeschrieben, daß bei Datenerhebungen auf die Rechtsgrundlage, welche die Datenerhebung rechtfertigt, oder andernfalls auf die Freiwilligkeit der Datenangabe hingewiesen wird.

Des weiteren wurde durch die verunglückte Gestaltung des Erhebungsbogens nicht verhindert, daß einzelne Fragen auch von den Betroffenen beantwortet werden, deren familiäre Verhältnisse am Stichtag klar und der Schule bekannt sind. In diesen Fällen war jedenfalls die Datenerhebung unzulässig, weil für die Aufgabenerfüllung der Schulverwaltung nicht erforderlich. Fragen nach dem Sorgerecht waren nur dann notwendig, wenn die Schüler noch nicht volljährig waren und die Eltern keinen gemeinsamen Hauptwohnsitz haben. Ebenfalls unzulässig, weil nicht erforderlich, war die Frage, ob die leibliche Mutter ledig ist. Gleiches gilt grundsätzlich für die Frage nach dem Zeitpunkt seit dem die Eltern verheiratet, geschieden, getrennt lebend oder verwitwet sind.

Die Landeshauptstadt München hat den Erhebungsbogen für Gastschülermeldungen entsprechend den vorgenannten Grundsätzen überarbeitet. Gegen die Neufassung bestehen aus datenschutzrechtlicher Sicht keine Bedenken.

13.4. Einsatz von Kleincomputern an der Schule

Der Einsatz von Kleincomputern an bayerischen Schulen soll neben der Verwendung des Computers im Unterricht von Anfang an auch die Möglichkeiten zur Unterstützung der an den Schulen anfallenden Verwaltungsarbeiten berücksichtigen. Um nun zu vermeiden, daß die gleichzeitige Verwendung der Kleincomputer zu Unterrichts- und schulischen Zwecken einen mißbräuchlichen Zugriff auf die Schulverwaltungsdaten eröffnet, hat das Bayerische Staatsministerium für Unterricht und Kultus an alle Schulen begrüßenswerte Hinweise zum Datenschutz gegeben. Das Kultusministerium hat insbesondere auf zwei Gesichtspunkte hingewiesen:

- Die Schülerdaten sind bei der elektronischen Speicherung vor dem Zugriff Unberechtigter zu schützen. Deshalb dürfen die Schulen Datenträger (Diskette, Platte, Band usw.) mit Schülerdaten ausschließlich für Zwecke der Schulverwaltung verwenden. Bei gleichzeitiger Benützung eines Datenträgers in der Schulverwaltung und im Unterricht könne nämlich nicht ausgeschlossen werden, daß findige Schüler selbst ein als sicher geltendes Paßwort sperren und Programmschutzmaßnahmen umgehen können.

- Auch bei der Weitergabe von Schülerdaten dürfe es zu keinem unberechtigten Zugriff kommen. Die Schulen dürfen daher personenbezogene Daten nicht mittels Datenfernübertragung oder per Band oder Diskette weitergeben.

Das Kultusministerium will mit diesen Weisungen auch den betroffenen Schülern und Eltern deutlich machen, daß auch im schulischen Bereich der Datenschutz bei Einsatz automatisierter Verfahren gewährleistet wird.

13.5. Hochschuldaten (Hochschulstatistik)

Im 6. Tätigkeitsbericht habe ich unter 4.5.6 berichtet, daß aufgrund des Volkszählungsurteils Erörterungen in Gang gekommen sind, ob und inwieweit das Hochschulstatistikgesetz abzuändern sei. Nach dem geltenden Hochschulstatistikgesetz können die für statistische Zwecke erhobenen Daten auch für Verwaltungszwecke der Hochschulen verwendet werden. Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer Konferenz am 16. Oktober 1984 in einem Beschluß ihre Auffassung zu einer Novellierung des Hochschulstatistikgesetzes dargelegt:

„1. Die Hochschulstatistik soll in ihren Erhebungsbereichen grundsätzlich nur noch bei den Hochschulen und deren Einrichtungen aufgrund vorhandener Verwaltungsdatenbestände mit Ausnahme der Prüfungsstatistik ohne Namen und Anschrift erhoben werden.

2. Auf eine Verlaufsstatistik soll verzichtet werden.

3. Das Erhebungsprogramm soll seinem Umfang nach gegenüber dem geltenden Hochschulstatikstikgesetz bereinigt und erheblich reduziert werden.

Die Datenschutzbeauftragten gehen davon aus, daß auch die Statistik der Prüfungskandidaten nicht personenbezogen erhoben werden muß. Sie würden es daher begrüßen, wenn in der Hochschulstatistik in ihrer Gesamtheit auf die Erhebung unmittelbar beim Betroffenen verzichtet würde.

Je mehr sich allerdings die amtliche Statistik auf Verwaltungsdaten gründet, um so mehr muß auf die Präzision der Befugnisnorm zur Datenerhebung im Hochschulrahmengesetz und in den Hochschulgesetzen der Länder geachtet werden. Die Verlagerung der Datenerhebung von der Statistik zur Verwaltung stellt vor allem die Landesgesetzgebung (das Landesrecht) vor neue Aufgaben. Nach Ansicht der Datenschutzbeauftragten muß nunmehr dort die Frage nach dem legitimen Umfang der Datenverarbeitung gestellt und beantwortet werden."

Die mittlerweile vorliegenden Entwürfe zum Hochschulstatistikgesetz sehen grundsätzlich keine Auskunftspflicht der Betroffenen mehr vor; vielmehr sollen statistische Daten künftig grundsätzlich nur noch bei den Hochschulen aufgrund der dort vorhandenen Verwaltungsdaten erhoben werden.

Das Bayerische Staatsministerium für Unterricht und Kultus erarbeitet derzeit einen Entwurf zur Novellierung des Bayerischen Hochschulgesetzes. Schwerpunkte der Überlegungen zu einer Novellierung des Bayerischen Hochschulgesetzes bilden dabei die gesetzlichen Regelungen zu

- der Erhebung und Verarbeitung von Daten durch die Hochschulen selbst,

- der Weitergabe dieser Daten an das Bayerische Landesamt für Statistik und Datenverarbeitung,

- der Weitergabe dieser Daten an das Bayerische Staatsministerium für Unterricht und Kultus,

- der Weitergabe dieser Daten an andere Stellen außerhalb der Hochschule und
- der Weitergabe personenbezogener Daten der Prüfungsämter an die Hochschulen.

Über das Bemühen des Bayerischen Staatsministeriums für Unterricht und Kultus, den datenschutzrechtlichen Belangen Rechnung zu tragen sowie die frühzeitige Beteiligung meiner Geschäftsstelle habe ich mich gefreut. In meiner Stellungnahme habe ich mitgeteilt:

Eine landesrechtliche Befugnis, nach der die Erhebung und Verarbeitung von personenbezogenen Daten zur Erfüllung der den Hochschulen nach dem Bayerischen Hochschulgesetz oder anderen Rechtsvorschriften obliegenden Aufgaben zulässig wäre, müßte erkennen lassen, um welche personenbezogenen Daten es sich handelt. Eine genauere Beschreibung könnte meines Erachtens auch in einer Rechtsverordnung erfolgen, für die dann in der Novelle des Bayerischen Hochschulgesetzes eine Rechtsgrundlage zu schaffen wäre.

Soweit an der zwangsweisen Datenerhebung festgehalten werden soll, müßten die Betroffenen bei der Datenerhebung auf die sie zur Auskunftserteilung verpflichtenden Rechtsvorschriften hingewiesen werden.

Gegen eine Vorschrift, die die Weiterleitung von Daten, die für Verwaltungszwecke der Hochschule erhoben wurden, an das Bayerische Landesamt für Statistik und Datenverarbeitung für statistische Zwecke vorsieht, habe ich keine grundsätzlichen Bedenken. Im Umkehrschluß zur Aussage des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 halte ich diese Nutzungsänderung verfassungsrechtlich für unbedenklich, da sie von der generellen Ausrichtung der Statistik her keine Beschwer erzeugt. Voraussetzung wäre aber auch insoweit die Schaffung einer Rechtsgrundlage, die dem Gebot der Normenklarheit und dem Verhältnismäßigkeitsgrundsatz entspricht.

Soweit in der Novelle des Bayerischen Hochschulgesetzes eine Rechtsgrundlage für eine Datenübermittlung der Hochschulen an das Bayerische Staatsministerium für Unterricht und Kultus erwogen wird, müßte diese in besonderer Weise sicherstellen, daß bei solchen Datenweitergaben keine unverhältnismäßigen Änderungen des Nutzungszwecks der Daten eintritt.

Für Datenweitergaben an andere Stellen als das Bayerische Landesamt für Statistik und Datenverarbeitung und das Bayerische Staatsministerium für Unterricht und Kultus habe ich keine Bedenken gegen eine Regelung entsprechend Art. 62 Abs. 2 des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen. Eine entsprechende Übermittlungsvorschrift ist nach den Darlegungen des Bayerischen Staatsministeriums für Unterricht und Kultus völlig ausreichend.

Ich hoffe, im nächsten Tätigkeitsbericht über das Gesetzgebungsverfahren berichten zu können.

13.6. Aushang von Klausurnoten

Aus dem universitären Bereich erreichen mich immer wieder Anfragen von Studenten, ob die Veröffentlichungen der Klausurnoten an allgemein zugänglichen Brettern im Universitätsbereich gegen datenschutzrechtliche Bestimmungen verstoßen. Hierzu ist grundsätzlich folgendes zu bemerken:

Die Veröffentlichung von Klausurnoten an allgemein zugänglichen Stellen der Universität ist datenschutzrechtlich als Übermittlung personenbezogener Daten an den Personenkreis zu werten, der von dem Aushang Kenntnis nehmen kann. Unabhängig davon, ob diese Noten unmittelbar aus einer Kartei entnommen worden sind und somit das Bayerische Datenschutzgesetz unmittelbar anwendbar wäre oder ob die Noten ausschließlich in Akten geführt worden sind, kann eine Veröffentlichung der Noten das Grundrecht auf informationelle Selbstbestimmung tangieren. Damit ist ganz allgemein datenschutzrechtlich zu prüfen, inwieweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und ob dadurch schutzwürdige Belange der betroffenen Studenten beeinträchtigt werden können.

Für die hier entscheidende Frage nun, ob durch den Aushang von Klausurnoten schutzwürdige Belange der Betroffenen beeinträchtigt werden, ist zu entscheiden, inwieweit die Noten durch andere Personen einem konkreten Studenten zuordnet und inwieweit dabei aus der Kenntnis der Daten belastende nachteilige Schlüsse für den Studenten gezogen werden können. Für die Frage der Schutzbedürftigkeit des einzelnen Studenten im Zusammenhang mit der Veröffentlichung seiner Daten kann nicht allein auf die Art der Daten abgestellt werden, vielmehr sind auch deren Nutzbarkeit und Verwendungsmöglichkeit durch Dritte zu berücksichtigen. Sollte daher die Veröffentlichung der Klausurnoten lediglich dem Zweck dienen, die einzelnen Teilnehmer einer Klausur vom Ergebnis zu unterrichten, und sollte gleichzeitig durch organisatorische Maßnahmen sichergestellt sein, daß durch die Art des Aushanges praktisch nur die Klausurteilnehmer den Bezug zu ihrer Person herstellen können, wäre die persönlichkeitsrechtliche Bedeutung der Klausurnote vergleichsweise gering. Weiterhin dürfte es eine Rolle spielen, ob die veröffentlichte Klausurnote ein relativ unbedeutendes Zwischenergebnis begrifft oder aber wesentlichen Einblick in das abschließende Prüfungsergebnis eines Studenten gibt. Im letzteren Falle könnte die Kenntnisnahme einer möglicherweise schlechten Note durch einen Unbeteiligten durchaus nachhaltige Auswirkungen auf die berufliche Laufbahn des Kandidaten haben. Dann würde bereits die Möglichkeit der Zuordnung der Daten zu einer bestimmten Person deren schutzwürdige Belange beeinträchtigen können und einen Aushang der Noten deshalb verbieten.

Auf die Entscheidung des BayVGH vom 12.3.1985, (Nr. 7 B 83 A. 563) weise ich hin, die sich mit der Bekanntgabe von Prüfungsnoten und den dabei zu wahrenden Belangen des Datenschutzes befaßt.

14. Archive

14.1. Notwendigkeit von Archivgesetzen

Die Schaffung von Archivgesetzen ist dringend. Hierauf habe ich bereits seit Jahren hingewiesen. Zum Regelungsbedarf habe ich mich insbesondere im 4. Tätigkeitsbericht

geäußert. Um deutlich zu machen, daß die Schaffung einer bloßen „Archivklausel" den Anforderungen einer Archivgesetzgebung nicht genügt, darf ich einige wesentliche Kernbereiche nochmals kurz ansprechen:

- Art. 20 Abs. 1 BayDSG legt den jeweiligen speichernden Stellen die Pflicht auf, personenbezogene Daten zu sperren, soweit die dort genannten Voraussetzungen erfüllt sind. Nach Art. 20 Abs. 4 sind die Daten sogar zu löschen. Art. 20 Abs. 3 gestattet der speichernden Stelle die Löschung personenbezogener Daten. Diese Bestimmungen werden zweifelsohne den Anforderungen der Archive nicht gerecht.

- Besondere Geheimhaltungsbestimmungen, wie etwa das Arztgeheimnis, das über den Tod hinaus gilt, das Steuer- sowie das Sozialgeheimnis, stehen in ihrer derzeitigen Ausgestaltung einer Archivierung durch zentrale Archive weitgehend entgegen.

- Die zeitgeschichtliche Forschung drängt zunehmend auf einen frühzeitigen Zugriff auf archiviertes Material. Der Gesetzgeber muß klare Maßstäbe für die Abwägung zwischen dem Grundrecht auf Wissenschaftsfreiheit und dem Schutz der Persönlichkeit schaffen und darf weder Gerichte noch die Archivverwaltung in diesem zunehmenden Spannungsverhältnis alleine lassen.

- Soweit die Archive Daten übernehmen, die bei Anwendung der Datenschutzgesetze aufgrund Sperrung oder Löschung der öffentlichen Verwaltung eigentlich entzogen sein müßten, ist die Aufgabe der Archive und deren eventuelle spätere Zusammenarbeit mit der öffentlichen Verwaltung exakt zu regeln. Die teilweise aus dem informationellen Selbstbestimmungsrecht der Bürger abgeleiteten Löschungsrechte dürfen nicht durch die Archivierung umgangen werden. Der im Einzelfall möglicherweise gleichwohl notwendige Zugriff der öffentlichen Verwaltung auf archivierte Akten muß deshalb gesetzlich geregelt werden.

- Bei der Datenübermittlung von personenbezogenen Daten an die Archivverwaltung genügt es seit 1. Januar 1983 nach dem ausdrücklichen Wortlaut des Bayerischen Datenschutzgesetzes nicht mehr, daß die personenbezogenen Daten zur Erfüllung öffentlicher Aufgaben der Archive notwendig sind, vielmehr muß diese Aufgabe der Archivverwaltung durch Gesetz zugewiesen sein (vgl. Art. 37 Abs. 3 i.V.m. Art. 17 Abs. 1 BayDSG). Dies gilt auch, wenn die Archive bereits vor einer endgültigen Archivierung bereit sind, Aktenmaterial zur Zwischenlagerung aufzunehmen, noch bevor über die endgültige Archivierung entschieden ist. Eine diesbezügliche Regelung besteht derzeit nur für die Meldedaten im Bayer. Meldegesetz (Art. 12 Abs. 2).

- Schließlich stellen bereits heute die neuen Informations- und Kommunikationstechniken die Archive vor bisher nicht bekannte Probleme. Wegen des sich ständig ändernden Datenbestandes in großen Datenbanken, der nicht unbedingt durch Akten oder sonstige Unterlagen später nachvollziehbar sein muß, wird es der Archivverwaltung möglicherweise zunehmend schwerfallen, heutige die Gesellschaft bewegende Erscheinungen (z. B. Befürchtungen wegen zunehmender Wirtschaftsspionage oder terroristischer Gewalttaten) für die Nachwelt nachzuzeichnen. Auch die Kommunikation wird derzeit allmählich vom Papier auf neue Kommunikationsmittel verlagert (vgl. z.B. den beginnenden Einsatz von TELETEX in der öffentlichen Verwaltung).

14.2. Bundesarchivgesetz-Entwurf

Zur Zeit liegt der Entwurf eines Bundesarchivgesetzes, Stand: 5.7.1984, vor (Bundesrats-Drucksache 371/84). Dieser Entwurf eines Bundesarchivgesetzes wird zweifelsohne auch für die Gesetzgebung in den Ländern Auswirkungen haben. So ist zu erwarten, daß bestimmte Regelungen über die Definition von Archivgut, dessen Abgabe an die Archive, dessen Benutzung sowie etwa die Schutzbestimmungen zugunsten Betroffener auch in die Diskussion um die entsprechenden Regelungen der Landesarchivgesetze einbezogen werden. Des weiteren enthält der Gesetzesentwurf wesentliche Öffnungsbestimmungen hinsichtlich verschiedener bundesrechtlicher Geheimhaltungsvorschriften, wie etwa das Steuergeheimnis und das Sozialgeheimnis, die für die entsprechende Archivierung der Landesarchive von maßgebender Bedeutung sind. Schließlich sieht der Gesetzesentwurf auch die Abgabe von bei Bundesbehörden angefallenem Archivgut an Landesarchive vor.

Welche Bedeutung die Länder diesem Bundesarchivgesetzentwurf beigemessen haben, läßt sich bereits aus der Stellungnahme des Bundesrates entnehmen, die über 20 Änderungswünsche enthält.

An dieser Stelle kann ich nicht auf Einzelheiten des Entwurfs eines Bundesarchivgesetzes eingehen. Auf die sich abzeichnende Problematik in Bezug auf die ärztliche Schweigepflicht (§ 203 Strafgesetzbuch) darf ich jedoch kurz hinweisen:

Der Bundesarchivgesetzentwurf versucht das Spannungsverhältnis zwischen den Ansprüchen einer historischen sowie einer zeitgeschichtlichen Forschung einerseits und dem Persönlichkeitsrecht der Betroffenen andererseits bezüglich der einer besonderen beruflichen Schweigepflicht unterliegenden Daten nach § 203 Strafgesetzbuch dadurch zu lösen, daß solche Daten dem Archiv grundsätzlich in anonymisierter Form angeboten werden sollen und die Nutzung von Archivgut unzulässig wäre, soweit die Geheimhaltungsvorschrift nach § 203 Abs. 1 oder 3 Strafgesetzbuch verletzt würde. Im Hinblick auf die Auswirkungen einer solchen Regelung für die Landesarchive ist zu berücksichtigen, daß solche der ärztlichen Schweigepflicht unterliegende Daten in erster Linie bei den dem Geltungsbereich eines Landesarchivgesetzes unterfallenden Krankenhäuser entstehen würden. Im Hinblick auf die Praktikabilität einer solchen Regelung muß daher ernsthaft geprüft werden, ob die vom Bundesarchivgesetzentwurf vorgesehene Anonymisierung als geeignetes Mittel in Betracht kommen kann. Der Vollzug dieser Bestimmung würde nämlich bei den in sehr großen Mengen anfallenden Daten in Krankenhäusern, Gesundheitsämtern, Beratungsstellen, Jugendämtern wohl zu großen praktischen Schwierigkeiten führen. Hierbei ist sowohl der personelle Aufwand zu berücksichtigen, den eine Anonymisierung erfordern würde, wie auch der Umstand, daß in solchen Unterlagen häufig auch auf Dritte Bezug genommen wird und bei einer Anonymisierung auch dieser Daten möglichweise der Akteninhalt unvollständig oder unverständlich würde.

Um zu vermeiden, daß unter Berufung auf den Persönlichkeitsschutz eine möglicherweise unpraktikable Regelung geschaffen würde, sollte als Alternative für den Verzicht auf eine Anonymisierung bei Übergabe der Daten an die Archive erwogen werden, ob nicht etwa ein verlängertes Benutzungsverbot solcher medizinischer Daten eine geeignetere Lösung wäre. Insoweit darf ich auf den in meinem letzten Tätigkeitbericht abgedruckten von den Datenschutzbeauftragten vorgelegten Entwurf eines Gesetzes über Sicherung und Nutzung von Archivgut unter § 8 Abs. 2 verweisen.

14.3. Bayerisches Archivgesetz – Sachstand

Leider hat sich der Sachstand bei den Arbeiten an einem Bayerischen Archivgesetz in den letzten Jahren nicht wesentlich verändert. Angesichts der Dringlichkeit eines Archivgesetzes sollte meines Erachtens die Schaffung eines Bundesarchivgesetzes, die sich möglicherweise noch längere Zeit hinziehen kann, nicht abgewartet werden. Allerdings muß ich mit Bedauern feststellen, daß etwa der Bayer. Städtetag nach wie vor ein Bayer. Archivgesetz ablehnt und lediglich einer aus meiner Sicht keineswegs ausreichenden Archivklausel den Vorzug geben würde.

Im Bayer. Senat ist die Dringlichkeit der Schaffung eines Gesetzes erkannt worden. Er hat am 10. Oktober 1985 folgenden begrüßenswerten Beschluß gefaßt:

> Die Bayerische Staatsregierung wird ersucht, alsbald einen Gesetzentwurf über die Sicherung und Nutzung von Archivgut in Bayern (BayArchivG) vorzulegen. Ein solches Gesetz ist für die Archive im Freistaat Bayern dringend erforderlich, da deren Aufgaben und Benutzung bislang nicht gesetzlich geregelt sind. Die derzeit bestehende Rechtsunsicherheit muß unverzüglich behoben werden, um die Funktion der Archive auch in der Zukunft zu sichern, um ferner einerseits das Persönlichkeitsrecht betroffener Personen zu wahren und andererseits den Zugang zu den Archiven klar zu regeln. Nicht zuletzt gibt eine gesetzliche Regelung den im Archivwesen tätigen Bediensteten einen deutlichen Handlungsrahmen. Hinsichtlich eines BayArchivG empfiehlt der Senat:
>
> 1. Auf die Verabschiedung eines Bundesarchivgesetzes durch den Bundestag kann nicht gewartet werden. Da ein derartiges Gesetz nur die Archive des Bundes und bundesrechtliche Vorschriften über Daten- und Geheimnisschutz betrifft, ist der bayerische Gesetzgeber nicht genötigt, auf den Erlaß dieses Bundesgesetzes zu warten. Zudem ist ungewiß, ob der 10. Deutsche Bundestag überhaupt das Gesetz noch verabschieden wird.
>
> 2. Ein BayArchivG sollte in erster Linie Aufgaben und Tätigkeit der staatlichen Archive sowie die Übernahme, Aufbewahrung und Benutzung des staatlichen Archivguts regeln.
>
> 3. Da die Tätigkeit sonstiger öffentlich-rechtlicher Archive (z.B. der gesetzgebenden Körperschaften, der Universitäten, Städte, Gemeinden, Landkreise und Bezirke) ebenfalls durch formelles Gesetz geregelt sein muß, empfiehlt es sich, im BayArchivG auch deren Bereich zu erfassen. Das Selbstverwaltungsrecht und auch die Besonderheiten und Traditionen solcher Archive lassen jedoch nicht zu, daß die Normen über die staatlichen Archive unmittelbar und ausnahmslos für die nicht-staatlichen Archive gelten. Vielmehr sollte ein eigener Abschnitt des Gesetzes den nicht-staatlichen Archiven gewidmet sein, der sich auf den Schutz der Persönlichkeit beschränkt und keine organisatorischen Bestimmungen enthält. Den Trägern der nicht-staatlichen Archive sollte die Ermächtigung erteilt werden, Besonderheiten ihres Archivgutes (z.B. Sperrfristen) generell, etwa durch Satzung (vgl. Urteil des Bayerischen Verwaltungsgerichtshofs vom 13.2.1985, DÖV 1985, S. 828 f.), anders zu regeln. Wegen der Unterschiedlichkeiten wäre ferner zu erwägen, hinsichtlich der gesetzgebenden Körperschaften, der Kommunen und der anderen Archive eigene gesetzliche Regelungen vorzusehen.

Ich würde es begrüßen, wenn diese Initiative zur Beschleunigung bei der Schaffung eines Bayerischen Landesarchivgesetzes beitragen würde.

14.4. Übergangslösung

Bis zum Inkrafttreten eines Landesarchivgesetzes müssen meines Erachtens bei der Einsichtnahme durch zeitgeschichtliche Forscher in archiviertes Material, das noch lebende Personen betreffen kann, folgende Mindestgrundsätze zur Beachtung des Grundrechts auf informationelle Selbstbestimmung beachtet werden:

- Die Einsichtnahme in archivierte Akten ist auf das für das jeweilige Projekt unbedingt erforderliche Maß zu beschränken. Dies ergibt sich aus dem Grundsatz der Verhältnismäßigkeit. Diese Beschränkung setzt aber voraus, daß die Zielsetzung eines Forschungsprojekts möglichst genau beschrieben wird.

- Soweit Forschungsvorhaben sich auf ethnische Gruppen beziehen, die aufgrund der jüngeren deutschen Geschichte als gefährdet angesehen werden müssen, sind besonders hohe Anforderungen an die Notwendigkeit des Forschungsvorhabens zu stellen. Gegebenenfalls sind hier Vertreter der betroffenen Gruppierungen zu beteiligen.

- Personenbezogene Daten, die aus Akten oder aus sonstigen im Rahmen des Forschungsvorhabens entstandenen Unterlagen entnommen sind, dürfen an Dritte nicht weitergegeben werden. Der Grundsatz der Zweckbindung ist auch gegenüber den an einem bestimmten Forschungsprojekt nicht beteiligten Mitarbeitern des gleichen Instituts anzuwenden. Daher ist auch jede Nutzung solcher personenbezogenen Daten durch die Forscher außerhalb des Forschungsprojekts ausgeschlossen.

- Die aus archivierten Akten entnommenen personenbezogenen Daten müssen vor Veröffentlichung des For-

schungsergebnisses durch die forschende Stelle so anonymisiert werden, daß ein Rückschluß auf bestimmte Personen nicht mehr möglich ist.

- Zur Überwachung der Einhaltung dieser zum Schutz des Persönlichkeitsrechts dienenden Auflagen ist rechtzeitig ein Pflichtstück der beabsichtigten Veröffentlichung an die Generaldirektion der Staatlichen Archive Bayerns abzuliefern.
- Vor einer erstmaligen Datenübermittlung an Forscher ist auch vom abgebenden Archiv zu prüfen, inwieweit die Forscher die Gewähr bieten, daß die genannten Auflagen eingehalten werden.

Durch diese Auflagen kann meines Erachtens in einer Übergangsphase sichergestellt werden, daß die zeitgeschichtliche Forschung ihrem zweifelsohne notwendigen Auftrag nachkommt und andererseits die Persönlichkeitsrechte eventuell Betroffener hinreichend gewahrt werden.

15. Straßenverkehr

15.1. Führerschein auf Probe

Durch Änderung des Straßenverkehrsgesetzes soll der „Führerschein auf Probe" als Teil eines Gesamtprojekts zur Erhöhung der Verkehrssicherheit eingeführt werden. Die Konzeption des Gesetzes sieht derzeit vor, alle Fahranfänger bis zum Alter von 25 Jahren für die Dauer einer 2-jährigen Probezeit zuzüglich einer 1-jährigen sogenannten Überliegefrist in einem beim Kraftfahrtbundesamt zu führenden Register zu erfassen. Das Register soll der Feststellung dienen, ob eine im Verkehrszentralregister eingetragene Straftat oder Ordnungswidrigkeit von einem Fahranfänger vor Ablauf der Probezeit begangen worden ist. Das Kraftfahrtbundesamt soll dann gegebenenfalls die für die entsprechenden Maßnahmen zuständige Führerscheinbehörde unterrichten, wenn der die mögliche Maßnahme auslösende Tatbestand erfüllt ist. Dieser Fall tritt z.B. dann ein, wenn von den Fahranfängern in einem besonderen Katalog aufgeführte Verkehrsstraftaten oder schwerwiegende Ordnungswidrigkeiten begangen worden sind. Die dann zu treffenden Maßnahmen können z.B. Nachschulungen oder die erneute Ablegung einer theoretischen Führerscheinprüfung bedeuten.

Nach dieser Konzeption entsteht allerdings eine zentrale Datei aller jungen Fahranfänger. Damit werden also auch jene Fahranfänger erfaßt, die während der Probezeit keinen Anlaß zu Maßnahmen gegeben haben. Selbstverständlich hat ein Datenschutzbeauftragter die Einrichtung einer solchen umfangreichen, sehr viele Bürger erfassenden zentralen Datei kritisch daraufhin zu prüfen, inwieweit ein solcher Eingriff gerechtfertigt ist. Hierbei ist insbesondere zu bedenken, daß auch der Gesetzgeber, der einen solchen Eingriff in die Bürgerrechte anordnet, den Grundsatz der Verhältnismäßigkeit zu beachten hat.

Bei Abwägung nach dem Verhältnismäßigkeitsgrundsatz ist demnach zwischen dem durch die zentrale Speicherung vorgenommenen Eingriff in die Rechte der Fahranfänger und den Interessen der Allgemeinheit nach einer maßgeblichen Erhöhung der Verkehrssicherheit abzuwägen. Dabei ist zu berücksichtigen, daß die aus der Unerfahrenheit und Risikobereitschaft resultierende hohe Unfallbeteiligung jugendlicher Fahranfänger empirisch-statistisch belegt ist. Weiter ist bekannt, daß auch die von jugendlichen Fahranfängern verursachten Verkehrsunfälle häufig überdurchschnittlich schwer sind und viele Menschenleben fordern. Die mit der Einführung des Führerscheins auf Probe beabsichtigten Maßnahmen sollen zum einen spezial-präventiv wirken, in dem sie erlauben, den durch schwere Verkehrsverstöße auffälligen Fahranfänger durch gezielte Maßnahmen zu einem verkehrsgerechten Verkehrsverhalten zu veranlassen. Zum anderen soll dieses Institut eine general-präventive Wirkung dadurch erreichen, daß die jugendlichen Fahranfänger ganz generell wegen der möglichen gegen sie zu ergreifenden Maßnahmen von einer besonders riskanten, die Verkehrsregeln mißachtenden Fahrweise absehen. Damit erscheint im Hinblick auf die notwendige Abwägung beim Grundsatz der Verhältnismäßigkeit die Geeignetheit der Maßnahmen zur Erhöhung der Verkehrssicherheit gewährleistet zu sein.

Bei der Abwägung zwischen der zu erzielenden Verkehrssicherheit und der möglichen Beeinträchtigung schutzwürdiger Belange durch die zentrale Speicherung auch korrekt fahrender Fahranfänger ist weiter zu prüfen, welche Maßnahmen der Gesetzgeber getroffen hat, um die durch eine zentrale Speicherung möglicherweise gegebenen Gefährdungen für das informationelle Selbstbestimmungsrecht auszuschließen. Weil eine solche Gefährdung insbesondere darin liegen könnte, daß die zentral gespeicherten Führerscheindaten für andere, den Einzelnen möglicherweise belastende Zwecke verwendet werden, ist zum einen durch ein strenges Verbot einer zweckwidrigen Nutzung und durch Schaffung ausreichender technisch-organisatorischer Maßnahmen ein gesetzeswidriger Mißbrauch zu verhindern. Im derzeit vorliegenden Entwurf hat der Gesetzgeber beide Anforderungen aufgenommen. Gegebenenfalls könnten diese noch verschärft werden.

Aus der Sicht des Datenschutzes erhebe ich daher gegen das Projekt „Führerschein auf Probe" nach dem derzeit vorliegendem Stand des Gesetzgebungsverfahrens keine Bedenken, weil der Entwurf zeigt, daß dem Grundsatz der Verhältnismäßigkeit durch weitgehenden Schutz der betroffenen Fahranfänger und durch geeignete Maßnahmen zur Erhöhung der Verkehrssicherheit hinreichend Rechnung getragen ist.

Die zeitweise diskutierte Alternative zu einer zentralen Speicherung der Führerscheinanfänger habe ich hingegen gerade aus datenschutzrechtlichen Bedenken abgelehnt. Diese Alternative hätte nämlich ein engmaschiges Netz der Kontrolle, eine wesentlich stärkere Belästigung der Bürger und vielfältige Datenflüsse erfordert und hätte außerdem eine Ungleichbehandlung der Bürger gleichwohl nicht vermeiden können. Weil diese meines Erachtens unpraktikable Lösung zeitweise gerade „aus Datenschutzgründen" favorisiert worden ist mit der Folge, daß der Datenschutz in Gefahr geraten ist, die notwendigen Bestrebungen zur Erhöhung der Verkehrssicherheit zu verhindern, habe ich mich mit Nachdruck gegen diese Alternative ausgesprochen. Datenschutz würde sich gerade bei dem Bürger, dem er dienen soll, ad absurdum führen, würden unter Berufung

auf ihn unpraktikable, den Interessen der Allgemeinheit wiedersprechende Lösungen nur um seiner selbst willen angestrebt.

15.2. Zentrales Verkehrs-Informationssystem (ZEVIS)

Das zentrale Fahrzeugregister beim Kraftfahrtbundesamt (KBA) hat einen Bestand von derzeit etwa 32 Mio. Fahrzeugen. Das Fahrzeugregister besteht aus Dateien der Fahrzeuge mit amtlichen Kennzeichen und der Fahrzeuge mit Versicherungskennzeichen. Durch das Zentrale Verkehrs-Informationssystem (ZEVIS) sollen Führung und Nutzung der Datenbestände beim KBA verbessert werden. Außerdem sind mit ZEVIS die technischen Möglichkeiten geschaffen worden, die Polizei online (Direktabruf) an die Datenbestände anzuschließen und Auskünfte im einstelligen Sekundenbereich zu geben. Hierauf wie auf die Tatsache, daß zur Schaffung der für die Einrichtung von ZEVIS erforderlichen Rechtsgrundlage ein Entwurf zur Änderung des Straßenverkehrsgesetzes vorliegt, habe ich in meinem letzten Tätigkeitsbericht ausführlich hingewiesen.

Zwar ist der jüngste Gesetzesentwurf zur Änderung des Straßenverkehrsgesetzes (Stand: 1.12.1984) ersichtlich von dem Bestreben getragen, den vom Bundesverfassungsgericht im Volkszählungsurteil entwickelten Grundsätzen für eine den Persönlichkeitsschutz wahrende verfassungsgemäße Erhebung und Verarbeitung personenbezogener Daten Rechnung zu tragen. Auch sind inzwischen einige Anregungen der Datenschutzbeauftragten berücksichtigt worden. Gleichwohl bestehen einige wesentliche datenschutzrechtliche Bedenken gegen den derzeit vorliegenden Entwurf. Dies gilt insbesondere für die sog. „P-Anfrage" im Direktabrufverfahren. Mit der „P-Anfrage" könnten die Polizeidienststellen – und zwar unabhängig vom Zweck der bloßen Identifizierung eines Fahrzeugs oder dessen Halters – generell erfahren, ob und gegebenenfalls welche verschiedenen Fahrzeuge auf eine bestimmte Person zugelassen und unter welcher Wohnanschrift diese Person gemeldet ist. Wie bereits im 6. Tätigkeitsbericht ausgeführt, ist das Risiko nicht völlig von der Hand zu weisen, daß das zentrale Fahrzeugregister sich zu einer Art „Bundes-Adressen-Register" entwickelt. Dies wäre jedenfalls mit den Zwecken eines zentralen Fahrzeugsregisters nicht mehr vereinbar und würde somit eine bedenkliche Zweckänderung darstellen. Ich hoffe jedoch, daß es im weiteren Verlauf der Beratung gelingen wird, die derzeit noch bestehenden datenschutzrechtlichen Bedenken durch entsprechende Änderungen des Gesetzesentwurfes noch auszuräumen.

16. Weitere Probleme in der Verwaltung

16.1. Einhaltung des „Dienstweges"

Das Bundesverwaltungsamt hatte ein bayerisches Gesundheitsamt um Auskunft über die gegenwärtige Anschrift eines Bürgers zur Erledigung einer Verwaltungsangelegenheit nach dem Bundesausbildungsförderungsgesetz gebeten.

Das Gesundheitsamt bat mich um Äußerung zu der Bitte des Bundesverwaltungsamts. Im Interesse einer möglichst guten Koordination von Fachinteressen und Anliegen des Datenschutzes habe ich das Bayerische Staatsministerium des Innern mit der Angelegenheit befaßt und Bedenken gegen die Weitergabe der Anschrift geäußert, weil damit möglicherweise eine Angabe über den Gesundheitszustand des Betroffenen weitergegeben würde, was unter dem Gesichtspunkt der ärztlichen Schweigepflicht zu prüfen wäre. Das Ministerium teilte diese Bedenken und hielt die Erteilung der Auskunft nicht für zulässig.

Die Angelegenheit war damit aber, zu meinem Bedauern, noch nicht abgeschlossen: Die zuständige Bezirksregierung, über die das Staatsministerium des Innern seine Beurteilung des Falles des Gesundheitsamt mitgeteilt hatte, rügte gegenüber dem Gesundheitsamt die unmittelbare Anfrage beim Landesbeauftragten für den Datenschutz.

Ich halte diese Vorgehensweise für unerfreulich, da sie dazu führen wird, den Landesbeauftragten für den Datenschutz von der Befassung mit Problemen, die bei den Behörden vor Ort im Bereiche des Daten schutzes auftreten, im Laufe der Zeit abzuschneiden. So selbstver ständlich es für den Landesbeauftragten für den Datenschutz sein muß, durch Beteiligung des jeweils zuständigen Ressorts die Berücksichtigung aller Umstände sicherzustellen, die bei der Beantwortung der zu lösenden Frage eine Rolle spielen, so selbst verständlich muß auch sein, daß die auf diese Weise eingeschalteten Behörden ihre über den Landesbeauftragten für den Datenschutz erlangte Kenntnis nicht dazu benutzen, die Personen oder Stellen, die sich an den Landesbeauftragten für den Datenschutz wenden, deswegen zu rügen. Gerade die unbürokratische Einschaltung meiner Dienststelle soll es ermöglichen, die mir vom Gesetz übertragene Kontrollaufgabe durch ebenso unbürokratische Beratung auszuüben. Dies setzt nicht zuletzt voraus, die in der täglichen Praxis auftretenden Datenschutzprobleme praxisnah zu bewerten und im Interesse aller Beteiligten, der Verwaltung ebenso wie der Bürger, zu lösen. Ein wesentlicher Zweck „Bayerischen Datenschutzes" könnte hier verloren gehen.

16.2. Ergänzung der staatlichen Vordruckrichtlinien um Hinweise auf den Datenschutz

Wie ich im 6. Tätigkeitsbericht ausführte, hatte ich in den Jahren 1982 und 1983 das für die staatlichen Vordruckrichtlinien zuständige Referat des Bayerischen Staatsministeriums des Innern gebeten, diese Richtlinien um eindeutige Hinweise zum Vollzug des Art. 16 Abs. 2 BayDSG zu ergänzen. Nach dieser Vorschrift des BayDSG muß der Betroffene bei der Datenerhebung auf die Vorschrift, die ihn zur Abgabe der Daten verpflichtet, oder auf die Freiwilligkeit der Angabe ausdrücklich hingewiesen werden. Das Bundesverfassungsgericht hat überdies im Volkszählungsurteil deutlich die Notwendigkeit herausgestellt, die Bürger darüber aufzuklären, für welche Verwendungszwecke Daten bei ihnen erhoben werden.

Die Vollzugsbekanntmachung zum BayDSG enthält zwar unter Nr. 16.4 Hinweise für die Behörden. Bei meinen Datenschutzkontrollen habe ich aber immer wieder festgestellt, daß Behörden nach wie vor im größeren Umgang Formulare verwenden, auf denen jeglicher oder aber ein ausreichender Hinweis zur Datenerhebung fehlt. Eine Ergänzung der staatlichen Vordruckrichtlinien durch entsprechende konkrete Anleitungen und Formulierungs-

vorschläge ist daher nicht nur im Interesse der Bürger, sondern auch der Verwaltung geboten. An den Richtlinien sollte auch klargestellt werden, daß die Hinweispflicht nach Art. 16 Abs. 2 BayDSG unabhängig davon gilt, ob im Zeitpunkt der Erhebung die Speicherung in einer Datei beabsichtigt ist.

Mit dem Staatsministerium des Innern wurden mehrere Gespräche geführt und Formulierungsmöglichkeiten besprochen. Das Ministerium hat im Sommer 1985 mitgeteilt, daß es eine entsprechende Ergänzung der staatlichen Vordruckrichtlinien vorbereitet.

16.3. Berücksichtigung des Datenschutzrechts im Vorbereitungsdienst der Rechtsreferendare

Wie schon im 6. Tätigkeitsbericht ausgeführt, hatte ich dem Bayerischen Staatsministerium des Innern vor längerer Zeit vorgeschlagen, nicht nur die Beamten des gehobenen Dienstes in ihrer Aus- und Fortbildung über Datenschutz zu unterrichten, sondern auch Rechtsreferendare im Rahmen ihres Vorbereitungsdienstes. Das Ministerium hatte seinerzeit die Regierungen auf mein Angebot, eine solche Unterrichtung durchzuführen, aufmerksam gemacht. Von diesem Angebot haben in der Zwischenzeit – mit einer Ausnahme – sämtliche Regierungen Gebrauch gemacht. An der in dem „fehlenden" Regierungsbezirk einmal (im November 1984) zustandegekommenen (halbtägigen) Fortbildungsveranstaltung „Datenschutzrecht", die nach den vorbereitenden Gesprächen auch zur freiwilligen Teilnahme für Rechtsreferendare vorgesehen war, nahm jedoch kein Rechtsreferendar teil. Angesichts des regen Interesses der Rechtsreferendare bei den anderen Regierungen sollte auch in diesem Regierungsbezirk eine entsprechende Veranstaltung ermöglicht werden.

17. Neue Medien

Mit dem Schlagwort „Neue Medien" werden eine Fülle neuer Informations- und Kommunikationstechniken sowie die mit Hilfe dieser neuen Techniken realisierbaren Nutzungsformen bezeichnet. Nach dem Bayer. Medienerprobungs- und -entwicklungsgesetz zählt hierzu die Verbreitung neuer Hörfunk- und Fernsehprogramme sowie die Veranstaltung rundfunkähnlicher Breitbandkommunikationsdienste. Zu letzteren gehören beispielsweise die Textdienste, wie die Kabeltextabruf- oder Kabeltextzugriffdienste sowie die Dienste, bei denen Bewegtbildangebote, Filme, Musik oder Sprechdarbietungen von einem Datenspeicher auf Anforderung an den Teilnehmer übermittelt werden. Schließlich zählen hierzu auch die Fernwirkdienste, bei denen ferngesteuert Messungen oder Beobachtungen über persönliche oder sachliche Verhältnisse eines Teilnehmers vorgenommen werden. Selbstverständlich gehört zu den Neuen Medien auch Bildschirmtext. Daneben wächst die Anzahl weiterer neuer Nutzungmöglichkeiten rapide. So hat die Deutsche Bundespost beispielsweise die Dienste TELEBOX und MAKATEL entwickelt. Zur Berliner Funkausstellung wird ein elektronisches Telefonbuch vorgestellt.

Um die weiteren Nutzungsmöglichkeiten im Bereich der neuen Medien erkennen und datenschutzrechtlich bewerten zu können, ist es wesentlich, die technischen Entwicklungen im Bereich der Telekommunikation zu beobachten. Hierzu zählen beispielsweise die Planung der Deutschen Bundespost zur Einrichtung eines Glasfaser-Overlay-Netzes sowie die in naher Zukunft bevorstehende Einführung der ISDN-Technik für zunächst Schmalband- und dann auch Breitbanddienste. Aber auch die Entwicklungen hin zum „elektronischen Büro" und etwa zur dezentralen Telearbeit sind zu berücksichtigen. Wegen der Breite der Palette sehe ich die Gefahr, daß die Datenschutzbeauftragten zunehmend in die Rolle von nur beobachtenden Statisten gedrängt werden und – in Anbetracht der knappen Personalkapazität – „ihrer Aufgabe", rechtzeitig die Datenschutzrechte der Bürger zu wahren, immer weniger nachkommen können.

Zunehmend wird jedenfalls deutlich, daß die allgemeinen Datenschutzgesetze den besonderen mit den Neuen Medien verbundenen datenschutzrechtlichen Risiken nicht gerecht werden. Meines Erachtens muß jedoch vor der Installation neuer Kommunikationstechniken und vor deren Nutzung ein ausreichendes Datenschutzinstrumentarium geschaffen werden. Inwieweit dies in einer alle Kommunikationsformen umfassenden „Telekommunikationsordnung" oder in einer Reihe von Einzelregelungen für die jeweiligen Kommunikationsdienste geschehen muß, muß sorgfältig geprüft werden. Jedenfalls sollte mehr als bisher bereits bei Konzeption neuer Techniken und deren Nutzungsmöglichkeiten an mögliche Auswirkungen auf die Persönlichkeitssphäre der Bürger geachtet werden.

17.1. Bildschirmtext

17.1.1. Zur Lage

Die Deutsche Bundespost hat im Berichtszeitraum den Betrieb von Bildschirmtext nach dem neuen CEPT-Standard endgültig aufgenommen. Allerdings haben sich die Zahlen der Bildschirmtext-Teilnehmer und der Anbieter nicht so entwickelt, wie dies zunächst von der Bundespost prognostiziert worden war. Derzeit (Stand: Juli 1985) gibt es in Bayern 3.779 Teilnehmer. Bundesweit – und damit grundsätzlich von bayerischen Teilnehmern aus ansprechbar – gibt es 3.800 Informationsanbieter im Bildschirmtext-System. 113 externe Rechner sind angeschlossen. Derzeit kommt die Mehrzahl der Bildschirmtext-Teilnehmer aus dem geschäftlichen Bereich. Der Anteil der Privaten beträgt nur etwa 10%.

Die Deutsche Bundespost plant für die nähere Zukunft eine Reihe von Systemverbesserungen: So soll die Bit-Rate bei der Übertragung auf 2.400 bit/sec. verdoppelt werden. Weiter soll die Möglichkeit der Einrichtung sog. „Mitbenutzer" bei den einzelnen Teilnehmern geschaffen werden. Familienmitglieder oder Arbeitnehmer hätten damit über einen Teilnehmeranschluß besser abgesicherte Zugangsmöglichkeiten. Auch sollen die Angebote künftig regionalisiert werden können. Des weiteren plant die Deutsche Bundespost den Verbund mit anderen Diensten. Beispielsweise soll ein Übergang zum französischen Bildschirmtext-System ermöglicht werden (siehe 17.1.4). Auch soll von Btx zu TELEX und TELETEX eine Verbindung beim Mitteilungsdienst geschaffen werden, um die Möglichkeiten beim Übermitteln von Mitteilungen zu verbessern. Schließlich soll für die fernere Zukunft durch die Einführung einer

Chip-Karte die Zugangssicherheit erhöht werden. Die Speicherung der bei Bildschirmtext anfallenden Nutzungsdaten soll ebenfalls im Laufe des nächsten Jahres verringert werden.

Zur Rechtssituation bei Bildschirmtext sind seit meinem letzten Tätigkeitsbericht keine wesentlichen Änderungen eingetreten. Wie bereits mitgeteilt, ist der Bildschirmtext-Staatsvertrag in Bayern am 1. September 1983 in Kraft getreten.

17.1.2. Probleme der Umsetzung der Datenschutzregelung im Staatsvertrag durch die Deutsche Bundespost

Zwischen den Ministerpräsidenten der Länder und der Deutschen Bundespost bestanden und bestehen Meinungsverschiedenheiten über die Reichweite der Geltung des Bildschirmtext-Staatsvertrages (Btx-StV) für die Deutsche Bundespost. Dies gilt auch für die in Art. 9 Btx-StV enthaltende Datenschutzregelung. In Kenntnis dieser Meinungsverschiedenheiten haben die Ministerpräsidenten und die Deutsche Bundespost letztlich die kompetenzrechtlichen Fragen bei Bildschirmtext ausgeklammert und einen Modus vivendi gefunden, der eine gegenseitige Respektierung der jeweiligen Rechtsauffassung vorsieht. Ein effektiver Datenschutz beim Bildschirmtext ist abhängig von diesem medienpolitischen Modus vivendi zwischen Bund und Ländern, der auf Konsens und gegenseitiges Verständnis angelegt ist. Allerdings waren auch die Unterzeichnung des Staatsvertrages und dessen Ratifikation durch die Länderparlamente davon abhängig, daß die Deutsche Bundespost den im Staatsvertrag geregelten Datenschutz einhalten und für ihren Bereich entsprechende Vorschriften erlassen werde. Jedenfalls wurden die diesbezüglichen Erklärungen der Deutschen Bundespost so interpretiert.

Bereits im letzten Tätigkeitsbericht hatte ich darauf hingewiesen, daß die zwischenzeitlich von der Deutschen Bundespost in die Fernmeldeordnung aufgenommenen Regelungen zu Bildschirmtext dem in Art. 9 Btx-StV erreichten Standard nicht entsprechen. Weil zudem die einzelnen für Bildschirmtext geltenden datenschutzrechtlichen Bestimmungen in der Fernmeldeordnung verstreut und nur schwer auffindbar sind, genügen die Bildschirmtextregelungen der Deutschen Bundespost auch nicht dem vom Bundesverfassungsgericht verlangten Gebot nach Normenklarheit und Transparenz.

Zwischenzeitlich hat die Deutsche Bundespost allerdings erklärt, daß sie die Bestimmungen über die Benutzung von Fernmeldedienstleistungen insgesamt zu überarbeiten und neu zu strukturieren beabsichtige. In diese Überlegungen seien auch die bereichsspezifischen Datenschutzregelungen bezüglich Bildschirmtext einbezogen. Dies begrüße ich außerordentlich. Meines Erachtens sollte eine solche Bildschirmtextregelung folgende Datenschutzgesichtspunkte ausdrücklich berücksichtigen:

- Die für den Betrieb von Bildschirmtext unerläßlichen Datenarten sind abschließend und aufgabenbezogen festzulegen. Dies gilt insbesondere für die Verbindungs-, die Abrechnungs- und die sonstigen Nutzungsdaten.
- Die Speicherung der in Art. 9 Abs. 3 Satz 1 Bildschirmtext-Staatsvertrag genannten Merkmale (Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von den einzelnen Teilnehmern in Anspruch genommenen Angebote) in Zusammenhang mit der Abrechnung ist ausdrücklich zu verbieten. Auch Umgehungsmöglichkeiten über die Nutzung mehrerer Leitseiten für das gesamte Angebot sind auszuschließen.
- Die personenbezogenen Daten, die für Abrechnungszwecke ausnahmsweise an den Anbieter übermittelt werden dürfen, sind einschließlich der Voraussetzungen ihrer Übermittlung abschließend und eindeutig festzulegen.
- Die Fristen, innerhalb deren die einzelnen bei der Nutzung von Bildschirmtext angefallenen personenbezogenen Daten gelöscht werden müssen, sind festzulegen.
- Bevor Daten für statistische Zwecke verwendet werden sollen, sind sie zu anonymisieren.
- Speicherung, Übermittlung und Löschung der bei Nutzung des Mitteilungsdienstes anfallenden Daten sind ebenfalls zu regeln.
- Inhalt und Umfang der Pflichten der Deutschen Bundespost zur Auskunft, Berichtigung, Sperre und Löschung sind festzuhalten.
- Die von der Deutschen Bundespost bei Betrieb von Bildschirmtext zu berücksichtigenden, notwendigen technisch-organisatorischen Maßnahmen sind, soweit dies nach dem jeweiligen Stand der Technik möglich ist, zu beschreiben.

Schließlich ist im Rahmen einer Normsetzung im Zusammenhang mit der Nutzung des Mediums Bildschirmtext vom Gesetzgeber noch folgendes Problem zu lösen:

Meines Erachtens muß der Gesetzgeber eindeutig feststellen, inwieweit das **Fernmeldegeheimnis** bei der Nutzung von Bildschirmtext beschränkt werden darf. Bei einer solchen Regelung ist zu berücksichtigen, daß, anders als beim herkömmlichen Brief-, Post- und Fernmeldeverkehr bei Bildschirmtext, Informationen aus breiten Lebensbereichen anfallen können, wie sie in dieser Fülle bei den bisherigen Postdiensten gebündelt kaum anzutreffen sind. Daher kann sich der Gesetzgeber meines Erachtens auch nicht darauf beschränken, das G 10-Gesetz einfach auf den Bildschirmtext für anwendbar zu erklären. Soweit überhaupt eine Beschränkung des Fernmeldegeheimnisses im Zusammenhang mit Bildschirmtext als unumgänglich notwendig erscheint, ist unter Abwägung des Verhältnismäßigkeitsgrundsatzes eine Einschränkung auf einige wenige im Gesetz ausdrücklich genannte Fälle zu begrenzen.

17.1.3. Datenschutzfragen beim technischen System-Konzept der Deutschen Bundespost

Unter dieser Thematik hatte ich in meinem 6. Tätigkeitsbericht insbesondere zwei Fragen angesprochen, den Umfang der Unterrichtung der Landesbeauftragten für den Datenschutz durch die Deutsche Bundespost und die Konzeption des Bildschirmtext-Systems bei der Abrechnung von Vergütungsdaten im Zusammenhang mit der Zuordnung mehrerer Leitseiten zu einem Angebot.

Unterrichtung

Die Unterrichtung der Datenschutzbeauftragten durch die Deutsche Bundespost hat sich im Berichtszeitraum wesentlich verbessert. So haben zusammen mit der Deutschen Bundespost in den letzten 12 Monaten zwei Informationsveranstaltungen stattgefunden, bei denen auch Einzelfragen des System-Konzepts von Bildschirmtext erörtert worden sind. Daneben konnte die Bildschirmtext-Leitzentrale in Ulm kurz besichtigt werden. Diese zunehmende Offenheit der Deutschen Bundespost begrüße ich. Ich sehe darin einen wesentlichen Schritt zu einer Normalisierung der Zusammenarbeit zwischen Deutscher Bundespost und den Landesbeauftragten für den Datenschutz. Ich gehe davon aus, daß noch bestehende Informationslücken geschlossen werden und die Deutsche Bundespost nicht durch unterschiedliche Informationszuteilung an den Bundesbeauftragten und die Landesbeauftragten für den Datenschutz zu erneuter Diskussion über die Fragen der Kompetenz bei Bildschirmtext Anlaß gibt. In diesem Zusammenhang darf ich darauf hinweisen, daß die Landesbeauftragten für den Datenschutz der Deutschen Bundespost gegenüber ausdrücklich deutlich gemacht haben, daß sie nicht beabsichtigen, Einrichtungen der Deutschen Bundespost zu prüfen. Dieser Verzicht bedeutete jedoch nicht, daß sie auf das Wissen verzichten wollen, das für die Prüfung der in ihrem Zuständigkeitsbereich liegenden Betreiber, Anbieter und Teilnehmer erforderlich ist.

Leitseiten- und Abrechnungsprobleme

Die Deutsche Bundespost gestattet es dem einzelnen Anbieter, sein Angebot auf bis zu 300 Leitseiten aufzuteilen. Wie ich bereits in meinem letzten Tätigkeitsbericht ausgeführt habe, hat dies zur Folge, daß bei entsprechender Aufteilung des Angebots die auf die Leitseiten bezogenen Abrechnungsdaten zumindest im Bereich der Deutschen Bundespost einen gewissen Rückschluß auf Art und Inhalt der abgerufenen Angebote zulassen. Dies ist nach dem Bildschirmtext-Staatsvertrag jedoch unzulässig.

Die Bundespost hat zu diesem datenschutzrechtlichen Problem folgendes mitgeteilt:

Als „Vergütungsdaten" werden von der Deutschen Bundespost neben der Teilnehmernummer das Datum, das Ende der Verbindung, die Leitseite des Anbieters sowie die Summe der während einer Verbindung unter der Leitseite eines Anbieters insgesamt aufgekommenen Vergütung gespeichert. Die Speicherung dieser Daten sei zum Zwecke der Einziehung der Vergütungsforderungen beim Teilnehmer durch die Deutsche Bundespost erforderlich. Die von der Bundespost gespeicherten Vergütungsdaten würden im Regelfall, d.h. bei Bezahlung durch den Teilnehmer zum fernmelderechtlich und fernmeldebetrieblich frühestmöglichen Zeitpunkt, spätestens jedoch nach 3 Monaten gelöscht. Lediglich bei Nichtzahlung des Teilnehmers müßten die Daten aus Beweisgründen bis zur endgültigen Erledigung des Zahlungsanspruchs gespeichert werden. Die nach erfolgloser Zahlungserinnerung durch die Deutsche Bundespost vorgesehene Weitergabe der Vergütungsdaten an den Anbieter beschränke sich jedoch auf weniger als 1% aller Abrechnungsvorgänge. Selbst in diesen Fällen erfahre der Anbieter lediglich Name sowie Anschrift des Teilnehmers, den Abrechnungszeitraum und die Summe der nicht gezahlten Vergütungen. Die Leitseiten, unter denen vergütungspflichtige Seiten vom Teilnehmer abgerufen worden seien, würden an den Anbieter nicht übermittelt.

Aus datenschutzrechtlichen Gründen habe ich aber die bisher bestehende Verknüpfung von Vergütungsdaten und Leitseiten jedenfalls im Verantwortungsbereich der Deutschen Bundespost als problematisch angesehen. Dies gilt nicht zuletzt, so lange noch nicht genügend Erfahrungen vorliegen, ob die Gerichte die im Bildschirmtext-Staatsvertrag vorgesehene und insoweit von der Deutschen Bundespost übernommene Abrechnungsregelung als ausreichend akzeptieren werden (siehe auch unten 17.1.4), und soweit von seiten der Bundesregierung vorgetragen wird, das G 10-Gesetz sei auch auf Bildschirmtext anwendbar.

Nun hat allerdings die Deutsche Bundespost erkennen lassen, daß sie bereit ist, das bisherige Verfahren zu ändern. So beabsichtigt die Post von der bisherigen Verknüpfung der Teilnehmernummer mit der Leitseite im Laufe des nächsten Jahres abzugehen und eine Verknüpfung nur noch zwischen Teilnehmer-Nummer und Anbieter herzustellen. Die Deutsche Bundespost wird somit das Abrechnungsverfahren in einen Stand versetzen, von dem bei Schaffung der Datenschutzregelung im Bildschirmtext-Staatsvertrag ausgegangen worden war.

17.1.4. Datenschutzprobleme in der Praxis

Zur Datenschutzregelung in Art. 9 Btx-StV hatte ich im 4. Tätigkeitsbericht geschrieben, daß viele meiner wesentlichen Datenschutzforderungen erfüllt sind, daß ich jedoch beispielsweise bei der Form der Abrechnung der bei Nutzung von Bildschirmtext angefallenen Gebühren und auch bei der im Gefolge von Vertragsabschlüssen zwischen Teilnehmern und Anbietern anfallenden Datenverarbeitung andere Lösungen vorgeschlagen hatte. Ich hatte daher angekündigt, daß ich die künftige Praxis bei Anwendung des Bildschirmtext-Staatsvertrag besonders aufmerksam verfolgen wolle. Soweit ich nun die bisherige Praxis des Bildschirmtext-Verfahrens beobachtet habe, sind mir jedenfalls hinsichtlich der Datenschutzregelung keine grundsätzlichen neuen Schwachstellen bekannt geworden, die eine kurzfristige Überarbeitung der Datenschutzregelung im Bildschirmtext-Staatsvertrag erforderlich machen würden. Gleichwohl sind mir folgende Punkte aufgefallen, die gegebenenfalls bei einer Novellierung von Art. 9 Btx-StV berücksichtigt werden sollten:

Kontrolltätigkeit

Im Rahmen der Überprüfung von Bildschirmtextseiten kann es im Einzelfall auch erforderlich sein, kostenpflichtige Seiten abzurufen. In Bayern wie in den meisten anderen Ländern hat die entsprechende Kontrollbehörde dem überprüften Anbieter die durch den Seitenabruf anfallenden Gebühren grundsätzlich zu ersetzen. Ich vertrete die Auffassung, daß im Zusammenhang mit der Überprüfung von Bildschirmtext-Anbietern die Kontrollbehörde nicht mit diesen Gebühren belastet werden sollte. Dies kann im Einzelfall dazu führen, daß von der Kontrolle eines Anbieters Abstand genommen werden muß, wenn er in seinem Angebot sehr viele und mit einer hohen Gebühr belegte Seiten eingestellt hat. In Anbetracht der derzeit noch geringen Anbieterzahl hat dieses Problem noch keine größere Bedeutung erlangt; dies kann sich jedoch möglichweise kurzfristig ändern. Meines Erachtens sollte daher bei Gelegenheit einer Novellierung des Bildschirmtext-Staatsvertrages die Gebührenfreiheit des Seitenabrufs für Kontrollzwecke festgeschrieben werden.

Ein weiteres Problem kann die Prüftätigkeit der für den Datenschutz zuständigen Kontrollbehörden bei Bildschirmtext erschweren: Damit eine Kontrolle effektiv sein kann, muß der Kontrolleur wissen, welche Stellen seiner Kontrolle unterliegen. Dies ist bei Bildschirmtext jedoch äußerst schwierig. Weder aus dem von der Bundespost herausgegebenen amtlichen Verzeichnis der Bildschirmtext-Teilnehmer noch aus dem Verzeichnis des elektronischen Suchbaumes läßt sich ohne größeren Zeitaufwand feststellen, welche meiner Kontrolle unterliegenden Bildschirmtext-Anbieter in Bayern ihren Sitz haben. Die Deutsche Bundespost hat auf entsprechende Bitten nach einem regional gegliederten Anbieterverzeichnis erklärt, daß derzeit jedenfalls die Erstellung solcher Verzeichnisse von ihr nicht vorgenommen werden könnte. Die Bundespost hat lediglich angeboten, eine Übersicht über alle im Bundesgebiet ansässigen Anbieter auf einen maschinenlesbaren Datenträger einem Bundesland zur Verfügung zu stellen, damit dieses gegebenenfalls dann auf Kosten der Länder derartige regionale Listen der Anbieter erstellen könnte. Die derzeitige Situation stellt einen für eine sinnvolle Kontrolle unhaltbaren Zustand dar.

Schließlich zeigt sich bezüglich der Kontrolltätigkeit noch ein weiteres Problem. Derzeit habe ich keine Rechtsgrundlage, um zu Kontrollzwecken das Angebot für sogenannte geschlossene Benutzergruppen einzusehen. Da diese geschlossenen Benutzergruppen jedoch möglicherweise einen sehr großen Personenkreis umfassen können, kann durchaus ein Bedürfnis bestehen, gelegentlich datenschutzrechtliche Prüfungen vorzunehmen. Auch hier sollten meines Erachtens bei Gelegenheit die entsprechenden gesetzlichen Regelungen geschaffen werden.

Gebührenabrechnung

Bei der Gebührenabrechnung sind mir keine Probleme bekanntgeworden. Wie oben bemerkt, werden derzeit die von der Post an die Teilnehmer gerichteten Abrechnungen für die kostenpflichtigen Bildschirmtextseiten nur in 1 % der Fälle nicht bezahlt. Inwieweit wegen dieser Vergütungsdaten inzwischen Gerichtsverfahren anhängig sind oder waren und inwieweit hierbei die Gerichte die nach dem Bildschirmtext-Staatsvertrag zugelassenen Beweisdaten für ausreichend erachtet haben, ist mir nicht bekannt. Diesbezüglich werde ich jedenfalls weiterhin beobachten. Sollten die Gerichte die aus Gründen des Persönlichkeitsschutzes nach dem Bildschirmtext-Staatsvertrag nur im geringem Umfang für den Nachweis des Abrufs von vergütungspflichtigen Seiten festgehaltenen Daten als nicht ausreichend bezeichnen, müßte an eine Novellierung des Bildschirmtext-Staatsvertrages gedacht werden. Allerdings dürfte diese nicht zu einer Erweiterung der Nutzungsdaten führen, da andernfalls die Probleme der Erstellung von Persönlichkeitsprofilen wieder aktuell würden. Vielmehr müßten dann die von den Datenschutzbeauftragen ursprünglich vorgeschlagenen Abrechnungsmodelle erneut in die Diskussion eingeführt werden.

Anschluß ausländischer Systeme

Der beabsichtigte Anschluß des deutschen Bildschirmtext-Systems an vergleichbare ausländische Systeme, wie dies mit dem französischen System für nächstes Jahr beabsichtigt ist, wirft aus der Sicht des Datenschutzes ebenfalls Fragen auf. Während nach dem für das deutsche Bildschirmtext-System geltenden Bildschirmtext-Staatsvertrag hinreichende datenschutzrechtliche Bestimmungen vorgesehen sind, die Anbieter wie Teilnehmer schützen sollen, fehlen in der Regel in ausländischen Systemen vergleichbare Bestimmungen zum Schutz der deutschen Bildschirmtext-Teilnehmer. Solange nicht beispielsweise durch zwischenstaatliche Abkommen sichergestellt ist, daß für den deutschen Teilnehmer auch in ausländischen Systemen grundsätzlich die gleichen Rechte gelten, muß dem Bildschirmtext-Teilnehmer durch einen unübersehbaren Hinweis deutlich gemacht werden, daß er zum einen das deutsche Bildschirmtext-System verläßt und in ein ausländisches eintritt, und daß zum anderen die ihm nach dem Bildschirmtext-Staatsvertrag zustehenden Rechte im ausländischen System nicht gelten. Sofern beispielsweise zu Abrechnungszwecken an ausländische Betreiber oder Anbieter wegen der Benutzung des ausländischen System Daten übermittelt werden sollen, darf dies bei der derzeit bestehenden Rechtslage nur mit Einwilligung des Betroffenen geschehen.

17.1.5. Prüfungserkenntnisse

Sind an das Bildschirmtextsystem externe Rechner angeschlossen, ist technisch nicht völlig ausgeschlossen, daß der Rechenzentrumsbetreiber die Benutzung des externen Computers protokolliert. Dies mag für den Teilnehmer solange ohne Bedeutung bleiben, solange er sich dem externen Rechner gegenüber nicht identifiziert hat. Will er aber beispielsweise nach einer Information über Warenangebote oder Urlaubsziele oder einer Kreditberatung in nähere Vertragsbeziehungen eintreten, etwa zur Bestellung einer Ware oder zur Buchung einer Reise, muß er sich identifizieren. Würde die bisherige Nutzung des Rechenzentrums aber protokolliert, wäre diese dem Teilnehmer nach seiner Identifizierung zuzuordnen.

Zusammen mit dem Bayer. Staatsministerium des Innern habe ich bei einem großen externen Rechner in Bayern einen Prüfbesuch abgestattet. Auf die entsprechenden Fragen wurde von dort versichert, daß das Teilnehmerverhalten bzw. der Dialog des Teilnehmers mit dem externen Rechner nicht protokolliert werde. Hierfür bestehe kein Interesse. Wieweit andere bayerische externe Rechner ähnlich verfahren, wird noch festzustellen sein.

Manche Anbieter, die externe Rechner an das Bildschirmtext-System angeschlossen haben, ermöglichen ihren Kunden eine Kontaktaufnahme allein durch Eingabe der Kundennummer. Daraufhin antwortet der externe Rechner mit Name und Anschrift des Kunden, der sich diese Dateneingabe etwa bei einer Bestellung ersparen kann. Gibt nun ein Dritter wahllos Kundennummern ein, wird er jeweils dann, wenn er durch Zufall eine richtige Kundennummer eingegeben hat, Name und Anschrift eines Kunden erfahren. Damit nun nicht die Tatsache, daß eine bestimmte Person Kunde eines Unternehmens und unter einer bestimmten Anschrift wohnhaft ist, oder gar der Kundenstamm insgesamt ausgeforscht werden kann, haben sich jedenfalls die größeren Versandunternehmen darauf geeinigt, auf Eingabe einer Kundennummer nicht mehr die vollständige Adresse auszugeben. In dem bayerischen Unternehmen, das ich zusammen mit dem Bayer. Staatsministerium des Innern aufgesucht hatte, wird inzwischen entsprechend verfahren. Ein Unbefugter kann mit den nun verkürzten

Daten wohl kaum einen Kunden eindeutig identifizieren und die Daten somit wohl nicht mißbrauchen.

17.2. Medienerprobungs- und -entwicklungsgesetz (MEG)

17.2.1. Datenschutz-Regelungen

Der Bayerische Landtag hat das Gesetz über die Erprobung und Entwicklung neuer Rundfunkangebote und anderer Mediendienste in Bayern am 15.11.1984 verabschiedet. Mit Ausnahme des 6. Abschnittes ist das Gesetz am 1.12.1984 in Kraft getreten. Datenschutzregelungen finden sich insbesondere in Art. 19 MEG bezüglich der Übermittlung der Rundfunksendungen und in Art. 31 mit 33 MEG bezüglich der „anderen Dienste", wie Textdienste, Bewegtbildangebote oder Fernwirkdienste. Diese Regelungen sind inhaltlich der Datenschutzvorschrift des Art. 9 Bildschirmtextstaatsvertrag stark angenähert, soweit nicht überhaupt auf diese Vorschrift verwiesen wird. Zwar sind in die Datenschutzregelungen im Bayer. Mediengesetz nicht alle meine Anregungen aufgenommen worden, doch zeichneten sie sich durch eine besondere Regelung zur Überwachung des Datenschutzes aus. Nach Art. 19 Abs. 2 und 3, Art. 31 Abs. 2 Satz 4 und Art. 32 Satz 2 MEG ist die Überwachung des Datenschutzes bei der Landeszentrale, den Kabelgesellschaften, den Betreibern (mit Ausnahme der Deutschen Bundespost) und den Anbietern dem Landesbeauftragten für den Datenschutz übertragen. Durch die Erweiterung der Überwachungstätigkeit des Datenschutzbeauftragten von öffentlichen auch auf die privaten Stellen wird dem verfassungsrechtlichen Erfordernis einer ausreichenden Datenschutzkontrolle in erfreulicher Weise Rechnung getragen. Eine Zersplitterung der Datenschutzkontrolle, wie sie im sonstigen Datenschutzrecht vorherrscht, hätte befürchten lassen, daß in dem erst allmählich sich verfestigenden Aufgabenbereich der Medienerprobung und -entwicklung eine wirklich effektive Datenschutzkontrolle nicht möglich sein wird. Mit diesem Schritt zur „Datenschutzkontrolle in einer Hand" ist Bayern meines Erachtens richtungsweisend in der deutschen Mediengesetzgebung.

Im übrigen darf ich darauf hinweisen, daß es gelungen ist, in den parlamentarischen Beratungen gegenüber dem Gesetzesentwurf der Staatsregierung zum MEG noch einige datenschutzrechtliche Verbesserungen einzubringen. Hierzu gehört unter anderem auch, daß Betreiber und Anbieter verpflichtet sind, dem Landesbeauftragten für den Datenschutz zur Erfüllung seiner Aufgaben jederzeit die kostenlose Kontrolle von Angeboten zu gewährleisten.

17.2.2. Abrechnung und wissenschaftliche Begleitforschung

Datenschutzrechtlich sind bei der Bewertung der Einführung neuer Rundfunkprogramme und anderer Dienste zunächst zwei Fragen von Interesse:

Fallen personenbezogene Daten durch eine bestimmte Nutzung der neuen Hörfunk- und Fernsehprogramme oder der sonstigen neuen Dienste an, die Rückschlüsse auf das Benutzerverhalten zulassen ?

Werden im Rahmen der wissenschaftlichen Begleitforschung personenbezogene Daten verarbeitet ?

Vor Beantwortung dieser Fragen ist zunächst auf den Stand der Verkabelung in Bayern, die Zahl der Projektteilnehmer und die Art der bisher angebotenen neuen Rundfunkprogramme und Dienste festzustellen:

- Die Bayer. Staatskanzlei hat mitgeteilt, daß es am 31.12.1984 in Bayern 272 Städte und Gemeinden mit Breitbandverteilnetzen gegeben habe. Bis zum 31.12.1985 beabsichtigt die Deutsche Bundespost in weiteren 140 bayerischen Städten und Gemeinden solche Netze anzulegen.
- Die Zahl der Projektteilnehmer liegt in München derzeit bei ca. 5.000 bis 6.000.
- Neben dem Angebot von einigen neuen Fernsehprogrammen sind im Rahmen des Pilotprojekts insbesondere eine Reihe von neuen Hörfunkprogrammen eingeführt worden. Andere Dienste werden derzeit meines Wissens noch nicht erprobt.

Aus datenschutzrechtlicher Sicht ist die Schaffung neuer Hörfunkprogramme kein Problem, weil hier keine benutzerbezogene **Abrechnung** entsteht. Aber auch die am Kabelpilotprojekt in München angeschlossenen Teilnehmer haben die von ihnen empfangenen Fernsehsendungen derzeit nicht sendungsbezogen abzurechnen. Vielmehr haben diese Teilnehmer einen Globalpreis von 16,25 DM neben der Rundfunkgebühr zu zahlen. Damit ist jedenfalls derzeit ein Rückschluß auf ein Nutzerverhalten über die Abrechnung nicht möglich.

Da insbesondere für die beabsichtigte Ausstrahlung von sogenannten „Pay-TV-Programmen" eine sendungsbezogene Abrechnung notwendig ist, werden auch in Bayern Überlegungen angestellt, auf welchem Wege diese geschehen kann. Derzeit werden auf dem Markt verschiedene technische Möglichkeiten angeboten, die je nach Ausgestaltung es einer Zentrale mehr oder weniger stark erlauben, das aktuelle Nutzungsverhalten der Teilnehmer festzustellen. Um hierbei eine Lösung zu erreichen, die den Persönlichkeitsschutz der Teilnehmer so wenig wie möglich beeinträchtigt, werde ich mich in die entsprechenden Beratungen in nächster Zeit einschalten.

Die **wissenschaftliche Begleitforschung** zum Kabelpilotprojekt wird weiter betrieben. Wie ich erfahren habe, bereitet die Medienkommission des Bundes derzeit im Rahmen der Medienerprobung die notwendigen Anbieteruntersuchungen vor. Die hierbei erarbeiteten Untersuchungsaufträge sollen wohl auch in Bayern als Grundlage für die wissenschaftliche Begleitung und Entwicklung neuer Rundfunkangebote herangezogen werden. Bislang liegen mir die entsprechenden Untersuchungsaufträge noch nicht vor. Ganz generell gilt jedoch, daß nach Art. 19 Abs. 1 Satz 1 MEG das Abfragen und das Verarbeiten personenbezogener Daten der Teilnehmer für Zwecke der wissenschaftlichen Begleitforschung im Rahmen des Medienerprobungs- und -entwicklungsgesetzes nur zulässig ist, wenn personenbezogene Daten hierzu erforderlich sind. Zunächst muß demnach geprüft werden, ob die Zwecke der wissenschaftlichen Begleitforschung im konkreten Fall nicht auch durch anonymisierte Daten erreicht werden können. Zwar wird vom MEG für die Datenerhebung zur wissenschaftlichen Begleitforschung nicht die Einwilligung der betroffenen Teilnehmer verlangt – wie dies in manchen anderen Mediengesetzen der Fall ist -, doch dürfte sich gerade im

Sinne einer vertrauensvollen Zusammenarbeit zwischen den Forschern und den Projektteilnehmern in vielen Fällen empfehlen, die Bürger wenn nicht schon ausdrücklich um ihre Einwilligung zu bitten, so sie doch zumindest über Sinn, Zweck und Notwendigkeit des Forschungsvorhabens und die dabei verarbeiteten personenbezogenen Daten zu unterrichten.

Nach Mitteilung der Projektkommission des Kabelpilotprojekts München liegen in Bayern noch keine Entwürfe zu einer Anbieteruntersuchung vor. Im übrigen wurde im Berichtszeitraum – aber noch vor Inkrafttreten des MEG – eine erste telefonische Akzeptanzuntersuchung einer relativ geringen Anzahl von Personen durchgeführt.

17.3. Fernwirkdienste

Die Bundespost bereitet die Einführung des Fernwirksystems „TEMEX" vor. TEMEX wird im wesentlichen über das herkömmliche Fernsprechnetz abgewickelt werden. Als dessen Anwendungsgebiete sind das Fernwirken und Fernmessen, Fernanzeigen, Fernschalten und Ferneinstellen vorgesehen. Über Möglichkeiten und Risiken von Fernwirkdiensten habe ich bereits ausführlich in meinem 6. Tätigkeitsbericht berichtet; im übrigen verweise ich bezüglich der technisch-organisatorischen Fragen auf Nr. 18.4.2.

Vor der Entscheidung über eine endgültige Einführung des TEMEX-Verfahrens plant die Bundespost System- und Betriebsversuche. Zweck der Systemversuche ist es, die Art der Dienstleistung dieses Fernwirksystems zur Debatte zu stellen und feststellen, ob ein derartiger Einsatz überhaupt sinnvoll ist und wieweit ein Bedarf dafür besteht. Dies soll unter Anwendung einer vereinfachten Technik geschehen, die nur Fernanzeigen und Fernschalten erlaubt und dabei nur die Übertragung zweiwertiger Informationen zuläßt. Hingegen soll mit den Betriebsversuchen die Technik des TEMEX-Verfahrens optimiert und erprobt werden. Ziel ist es, möglichst viele Anwendungsformen und -arten auf ihre Tauglichkeit zu prüfen.

Systemversuche haben in München und Ludwigshafen begonnen. Die insgesamt vorgesehenen 8 Betriebsversuche werden wohl erst im Jahr 1986 starten.

Bei den Systemversuchen in München und Ludwigshafen sollen jeweils nicht mehr als 400 Nutzer teilnehmen. Gegebenenfalls wird diese Zahl auf mehrere Anbieter aufgeteilt. Derzeit ist in München zwar die Installation der zentralen TEMEX-Einrichtung abgeschlossen, doch sind bisher erst einige Nutzeranschlüsse eingerichtet. Als Anbieter werden zunächst Bewachungsunternehmen auftreten.

Bei dem Betriebsversuchen hingegen soll die Nutzerzahl nach oben weitgehend offen sein. Endgültige Festlegungen liegen noch nicht vor.

Datenschutzrechtliche Überlegungen

Während der Systemversuche werde ich im Rahmen meiner Möglichkeiten auch eventuelle Auswirkungen auf die Persönlichkeitsrechte der Anbieter und Nutzer beobachten. Mit der Deutschen Bundespost, die sich beim Dienst „TEMEX" sehr kooperativ zeigt, habe ich einen engen Kontakt für die Zeit der Systemversuche vereinbart.

Im übrigen hat die Deutsche Bundespost in den Vordrucken für die Mustervereinbarungen mit Anbietern und Nutzern im Systemversuch festgelegt, daß der Anbieter von Fernwirkdiensten durch TEMEX vermittelte personenbezogene Daten Dritter nur dann speichern und weiterverarbeiten darf, wenn der Betroffene den Verwendungszweck dieser Daten und die Wirkungsweisen dieses Dienstes kennt und mit der Speicherung und der Weiterverarbeitung einverstanden ist. Von der Deutschen Bundespost werden nach deren eigener Erklärung keine personenbezogenen Daten bei der Übermittlung von Fernwirkinformationen durch TEMEX-Dienstleistungen in vereinfachter Technik gespeichert.

Um Befürchtungen entgegenzutreten, daß über TEMEX-Abrufe ein Persönlichkeitsbild der Nutzer erstellt werden könne, erwägt die Deutsche Bundespost für die Zukunft, gegebenenfalls nur maximal 4 Abfragen im Monat zuzulassen. Möglicherweise werde sie auch als weiteren Dienst anbieten, daß nicht der Anbieter, sondern die Post beim Nutzer die Abfragen durchführe. Damit wären wohl die Risiken ausgeschlossen, daß durch unkontrolliertes Abfragen von Informationen beim Teilnehmer dessen Nutzungsverhalten beispielsweise über den Strom- oder Wasserverbrauch festgestellt werden könnte.

Die Deutsche Bundespost hat in Besprechungen darauf hingewiesen, daß die von seiten des Datenschutzes erhobene Forderung, daß auch bei endgültiger Einführung der Technik die Teilnahme am Dienst absolut freiwillig sein müsse und die jederzeitige Abschaltbarkeit zu gewährleisten sei, auf Probleme stoße. In diesem Zusammenhang müsse gegebenenfalls erörtert werden, inwieweit ein Anschluß- und Benutzungszwang beispielsweise bei der Ablesung von Wärmeeinheiten durch Energieversorgungsunternehmen vom Bürger hingenommen werden müsse. Zu prüfen werde auch sein, inwieweit dies gegebenenfalls in den jeweiligen Benutzungsverträgen verankert werden könne. Bei der Frage der jederzeitigen Abschaltbarkeit des Fernwirkdienstes – im Bayer. Mediengesetz ist diese Möglichkeit anders als in Berlin nicht gesetzlich vorgesehen – wurde von der Post die Frage aufgeworfen, inwieweit diese Forderung auf besonders „riskante" Dienste beschränkt werden sollte. Dies könnten etwa solche Dienste sein, über die beispielsweise eine Wohnung rund um die Uhr bewacht werde, bei denen der betroffene Bürger aber gegebenenfalls die Möglichkeit haben müsse, sich zeitweise der „Bewachung" bewußt zu entziehen.

Systemmöglichkeiten

Für die Einsatzmöglichkeiten der einzelnen TEMEX-Dienste ist es entscheidend, welche „Schnittstellen" im Einzelfall gewählt werden. Die Post möchte weitgehend flexibel sein und den Anbietern und Nutzern die Möglichkeit geben, sich für eine bestimmte Nutzungsform des TEMEX-Dienstes zu entscheiden. Diese mögliche Entscheidung kann auch aus der Sicht des Datenschutzes von Bedeutung sein, weil manche zumindest theoretisch möglichen Risiken bei der Wahl bestimmter Schnittstellen von vorneherein weitgehend ausgeschlossen sein dürften. So bietet die Post Schnittstellen an, die lediglich die Übertragung von einer 1-Bit-wertigen Information in eine Richtung zulassen. Ein „Ausforschen" des Nutzers ist hier weitgehend ausgeschlossen. Andererseits bietet die Post auch Schnittstellen an, über die etwas mehr Daten abgefragt werden können.

Die System- und Betriebsversuche werden den Datenschutzbeauftragten auch Informationen darüber vermitteln, für welche Dienste welche Schnittstellen ausreichend sind. Dann können die Datenschutzbeauftragten ggf. künftig bei den Anbietern darauf hinwirken, nur die jeweils für den beabsichtigten Einsatz ausreichende Technik zu wählen.

Vertragslösung

Zur Durchführung der TEMEX-Systemversuche hat die Deutsche Bundespost – wie oben bemerkt – Mustervereinbarungen vorbereitet, die zwischen ihr und den jeweiligen Anbietern, bzw. Nutzern des Fernwirkdienstes abgeschlossen werden. Damit werden die Rechtsbeziehungen zwischen der Deutschen Bundespost und den Teilnehmern auf eine vertragliche Grundlage gestützt. Die Bundespost hat die zur datenschutzrechtlichen Verbesserung von mir vorgetragenen Anregungen in die Mustervereinbarungen übernommen.

Datenschutzkontrolle

Derzeit kann ich noch nicht endgültig absehen, inwieweit neben privaten Anbietern auch öffentliche Stellen als Anbieter des TEMEX-Systems auftreten werden. Ich gehe davon aus, daß ich unabhängig von den für den Systemversuch gewonnenen Anbietern auch im Hinblick auf die weitere Entwicklung des TEMEX-Systems bei der Datenschutzkontrolle eingeschaltet werde.

18. Technischer und organisatorischer Bereich

18.1. Technische und organisatorische Grundsatzfragen

18.1.1. Anforderungen an die Protokollierung von Ablaufdaten für Revisionszwecke beim Einsatz von DV-Systemen mittlerer Größe

Im 6. Tätigkeitsbericht wurden unter der Textziffer 5.1.1 auf Seite 76 Ausführungen über Grundsätze zur Revision der Datenverarbeitung gemacht. Die Anforderungen haben vor allem für die Groß-EDV Bedeutung.

Anders als in der Groß-EDV oder in Mehrzweckrechenzentren, wo die Zahl der Nutzer öfter wechselt, sind beim Einsatz von DV-Systemen mittlerer Größe, die häufig als dedizierte Systeme zum Einsatz kommen, reduzierte Anforderungen an den Umfang der Aufzeichnungen von Ablaufdaten zu stellen, weil ein mit den SMF-Sätzen (SMF = System Management Facility) bei IBM-MVS-Systemen vergleichbarer Protokollierungsaufwand hier unverhältnismäßig wäre. SMF schreibt von jeder DV-Aktivität einen Protokollsatz.

Als Betriebsbedingungen für DV-Systeme mittlerer Größe werden angenommen:

- Die Nutzer der DV-Anwendung bedienen sich der sog. Menuetechnik an Bildschirmen: Jedem Nutzer ist ein Benutzerprofil, das heißt die Menge der Aufgaben, zu deren Ausführung er berechtigt ist, zuzuordnen. Vor dem Aktivwerden muß er sich durch seine Benutzerkennung und sein persönliches Kennwort gegenüber dem System identifizieren. In der Regel bekommt der Nutzer dann im Menue nur solche Dienste (Transaktionen) angezeigt, zu deren Ausführung er berechtigt ist.
- Sofern die Verfahrenserstellung selbst erfolgt, sind dafür bestimmte Personen (Programmierer, Systemspezialisten o.ä.) zuständig. Diese Personen greifen bei der Programmerstellung und -wartung auf eigene Bibliotheken (Programme und Daten) zu und haben in der Regel keinen Zugriff auf Produktionsprogramme und -daten. Beim Einsatz von Hersteller- oder Fremdsoftware ist der Quell-Code (SOURCE-Code) von der Anlage zu entfernen, damit unkontrolliert keine Modifikationen, die der Transparenz der eingesetzten Programmversionen abträglich wären, vorgenommen werden können.
- Der oder die Systemverantwortlichen richten Benutzerprofile ein und verwalten die Systembibliothek. Sie sind für die Installation neuer Programme und Programmversionen zuständig. Revisionsfähige Unterlagen liegen hierüber dann vor, wenn erkennbar ist, daß die augenblicklich gespeicherte Programmversion mit der freigegebenen Programmversion identisch ist. Das geschieht in der Regel über maschinell vergebene eindeutige Versionsnummern, die das Entstehungs-/Änderungsdatum enthalten sollen. Eine Freigabe ist auch bei Programmänderungen erforderlich.
- Das DV-System arbeitet als autonomes System und ist mit anderen Systemen nicht vernetzt („stand alone System"). Besteht ein Kommunikationsverbund mit anderen Systemen, was durchaus vorkommen kann, sind das Netz und die möglichen Datenströme zu dokumentieren.
- Für die DV-Anwendungen, die im Stapelbetrieb ablaufen, existiert entweder ein Terminplan oder der Systemverantwortliche prüft vor jedem Lauf eines Batch-Programmes die Zulässigkeit.

Für Zwecke der Revision sind bestimmte Ablaufdaten maschinell aufzuzeichnen. Grundsätzlich ist anzustreben, daß die Aufzeichnungen auf bestimmte (sensible) Tätigkeiten/Anwendungen beschränkt werden können. Festzuhalten sind zumindest alle Aktivitäten, die von der Norm abweichen. Ein Anmelden eines Benutzers über Datensichtstation an eine Anwendung im Rahmen seines Berechtigungsprofils braucht jedoch nicht unbedingt protokolliert zu werden, da diese Informationen, so nützlich sie auch im Einzelfall sein mögen, die Protokolldatei überfrachten und die Auswertbarkeit, die häufig manuell erfolgen muß, weil eine geeignete Auswertesoftware nicht zur Verfügung steht, beeinträchtigen.

Zum Nachweis eines ordnungsgemäßen DV-Betriebes gelten als Mindestanforderungen:

- Dokumentation der Benutzerprofile (der Zeitpunkt der Generierung sowie eventuelle Änderungen müssen ersichtlich sein);
- Dokumentation der DV-Verfahren;
- Dokumentation der Kommunikationsverbindungen, sofern vorhanden;
- Aufzeichnungen über wesentliche DV-Aktivitäten, dazu gehören (mit Zeitstempel – Datum, Uhrzeit, Veranlasser):
  - Starten und Beenden des Systems,
  - Starten und Beenden der Dialoganwendungen,

- Alle Eingriffe des/der Systemverantwortlichen sowie der/des Maschinenbediener/s in das DV-System,
- Zugriff auf bestimmte Produktionsbibliotheken (Programme und Daten), insbesondere von Batch-Programmen,
- Eingriffe in das SPOOLING,
- Alle festgestellten Sicherheitsverfehlungen,
- Alle abnormalen Programmbeendigungen, soweit sie sich auf die Verarbeitung mit Produktionsdaten beziehen,
- Eingriffe der Wartung, insbesondere der Fernwartung,
- An-/Abschaltung von Leitungen.

Die Aufzeichnungen müssen vollständig und zwangsläufig sein. Ein Zugriff auf die Protokolldatei darf nur autorisierten Personen erlaubt sein und ist ebenfalls zu protokollieren. Ein Manipulationsversuch in der Protokolldatei muß unbedingt Spuren hinterlassen. Außerdem muß aus den Aufzeichnungsdaten ersichtlich sein, welche Protokollierungsfunktionen generiert sind bzw. welche (auch nur kurzzeitig) abgeschaltet wurden.

Die Aufzeichnungen sind regelmäßig (z.B. wöchentlich) nach

- Sicherheitsverletzungen
- abnormalen Job/Programm-Beendigungen
- Zugriffen auf bestimmte, sensible Produktionsdateien von Batch-Anwendungen oder Dienstprogrammen

auszuwerten. Die Auswertung ist dann effektiv, wenn sie maschinell erfolgt.

Die Protokollinformationen sind mindestens ein Jahr aufzubewahren und sollen in erster Linie einen Nachweis für ein ordnungsmäßiges Verhalten des/r Systemverantwortlichen darstellen.

Leider sind für solche umfassenden Vorstellungen nur vereinzelt Ansätze zu finden. Mit der Zunahme der Leistungsfähigkeit der DV-Anlagen dürfte das oft entgegengehaltene Argument, daß die Aufzeichnung von Ablaufdaten den Durchsatz behindere, immer mehr an Glaubwürdigkeit verlieren. Die Hersteller sind aufgerufen, auch auf DV-Anlagen mittlerer Größe etwas mehr für die Transparenz der Datenverarbeitung zu tun.

18.1.2. Individuelle Datenverarbeitung

Die herkömmliche elektronische Datenverarbeitung war dadurch geprägt, daß die anfallenden Tätigkeiten, wie Datenerfassung, Programmierung, Systemverwaltung, Maschinenbedienung, Arbeitsvor- und -nachbereitung, Datenträgerverwaltung, Dateneingabe und Sachbe arbeitung unterschiedlichen Personen und Organisationseinheiten übertragen wurden. Diese Funktionstrennung erhöhte die Sicherheit der Datenverarbeitung vor Mißbrauch. Die individuelle Datenverarbeitung (IDV) ist dadurch gekennzeichnet, daß viele dieser Tätigkeiten von ein- und derselben Person erledigt werden. Diese Entwicklung hat ihren Ursprung in der Miniaturisierung der Computerbauteile und der damit verbundenen Leistungsexplosion. So ist es heute möglich, Kleincomputer mit dem Leistungspektrum früherer Großrechner zu bauen. IDV kann beispielsweise mit Personal Computern bzw. Small-Business Computern (Arbeitsplatzcomputern) betrieben werden. Diese Geräte können autonom (im stand-alone-Betrieb), vernetzt oder als Terminal mit Anschluß an einen Großrechner eingesetzt werden.

Der Preisverfall dieser Geräte war in den letzten Jahren beträchtlich. Trotzdem ist ihr Verbreitungsgrad in der öffentlichen Verwaltung noch gering, wenn man vom Schulbereich absieht, wo Mikrocomputer seit Jahren im Informatikunterricht und für Zwecke der Schulverwaltung, wie Zeugnisschreibung und Erstellung von Schülerlisten, Verwendung finden. Die Bedeutung dieser Minicomputer wird in den nächsten Jahren zunehmen. Die Revision beobachtet die Entwicklung der IDV mit Unbehagen, da es in der IDV noch weniger Unterlagen gibt, die eine DV-Revision unterstützen. In der Fachpresse war zu lesen, daß in der Bundesrepublik 1984 etwa 500 000 Personal Computer abgesetzt wurden. Ein nicht unbedeutender Prozentsatz davon dürfte in den privaten Haushalten stehen.

Angesichts dieser Entwicklung bin ich mit der berechtigten Frage konfrontiert worden, wie der Einsatz privater Computer (Homecomputer) für dienstliche Tätigkeiten kontrollierbar ist. Probleme bei der Kontrolle der Datenverarbeitung kann es auch geben, wenn der Bedienstete seinen eigenen Personal Computer in die Dienststelle mitbringt und dienstliche Tätigkeiten darauf verrichtet.

Weitere Risiken beim Einsatz von Personal Computern sind:

- Mangelhafte Standardsoftware zur Prüfung der Zugriffsberechtigung und das Fehlen von maschinellen Protokollierungseinrichtungen über die Benutzung des Personal Computers,
- Bedienung des Personal Computers durch wenig geschultes Personal,
- Arbeiten mit selbstentwickelten Programmen, die mangelhaft ausgetestet wurden,
- Mangelhafte Dokumentation der Programme und Verfahren,
- Auftreten erhöhter Abstrahlwerte, insbesondere des Bildschirmes und des Druckers, so daß die dargestellte und ausgedruckte Information von Unberechtigten empfangen werden kann.
- Darüber hinaus kann der Benutzer gespeicherte Daten auch auf eine Diskette oder ein Streamer Tape kopieren und an Nicht-Befugte weitergeben oder einzelne Datenträger – auch nur zeitweise – austauschen.

Die Kontrollierbarkeit der Individuellen Datenverarbeitung wurde bereits in vielen Gremien erörtert. Lösungsmethoden für dieses Problem gibt es nur ansatzweise. Man hat erkannt, daß sich die Risiken durch den Personal Computer allgemein, insbesondere aber durch eine Vernetzung untereinander und den Anschluß an einen Großrechner erhöhen. Eine Orientierungshilfe, die Mißbrauchsmöglichkeiten aufzählt und Sicherungsmaßnahmen vorschlägt, ist in Bearbeitung. Dabei ist grundsätzlich zwischen Mißbrauchsmöglichkeiten durch Außenstehende und durch Benutzer zu unterscheiden.

Bezüglich der Sicherungsmaßnahmen ist folgendes festzustellen:

- Die Individuelle Datenverarbeitung sollte nur nach einer ausdrücklichen, besonderen Erlaubnis gestattet werden. Dort sind die Anwendungsgebiete, Zuständigkeiten und Verantwortlichkeiten festzulegen.
- Die Benutzung von privaten Geräten am Arbeitsplatz und die Mitnahme dienstlicher Geräte nach Hause, um dienstliche Aufgaben außerhalb des Arbeitsplatzes zu bearbeiten, sollte aus Gründen der Transparenz und Kontrollierbarkeit bei der Verarbeitung personenbezogener Daten nur in Ausnahmefällen gestattet sein.
- Der Zugang zum Personal Computer ist mechanisch zu sichern.
- Datenträger und Ausdrucke sind verschlossen aufzubewahren.
- Die Benutzung eines Personal Computers durch Unbefugte ist durch eine Identifizierungs- und Authentifikationsprozedur zu verhindern. Bei längeren inaktiven Zeiten ist in den Logoff-Zustand zu verzweigen.
- Sensible Daten sind in verschlüsselter Form abzuspeichern. Sie sind dann nur solchen Personen zugänglich, die den Entschlüsselungscode kennen. Entsprechende Standardsoftware ist mittlerweile erhältlich.
- Standardsoftware darf nicht verändert werden.
- Selbstgeschriebene Programme sind ausreichend zu dokumentieren.

Schließlich sollte die IDV nur dort eingesetzt werden, wo sie nach Art der Aufgabenstellung zweckmäßiger oder wirtschaftlicher als die bisherige Verfahrensweise ist.

18.1.3. Elektronisches Büro

Moderne digitale Nebenstellenanlagen werden häufig wegen ihrer erweiterten Kommunikationsfunktionen als erster Schritt in die Richtung zu einem elektronischen Büro angesehen. Neben den Funktionen zur Unterstützung des Fernsprechverkehrs im Nebenstellenbereich, wie Dreierkonferenz, selbsttätiger Rückruf, Rufumleitung, Anklopfen, Personensuche und Kurzwahl, können moderne Nebenstellenanlagen aufzeichnen, wer wann wie lange mit welcher Rufnummer in Verbindung gestanden hatte. In früheren Tätigkeitsberichten ist über das Problem der Gesprächsdatenerfassung bereits berichtet worden. Inzwischen bieten moderne Systeme eine Reihe von entsprechenden Funktionen. Erst durch das Eintasten eines persönlichen geheimen Identifikationscodes erhält ein Teilnehmer einer modernen Nebenstellenanlage Zugang zu einer Amtsleitung, die aus dem Nebenstellenbereich herausführt. Durch diesen Identifikationscode läßt sich ein Gespräch eindeutig dem Verursacher zuordnen. Manche Fernsprechapparate sind auch schon mit einer technischen Einrichtung ausgestattet, die den Apparat zur Benutzung erst dann freigibt, wenn eine gültige Chipkarte eingelegt wurde. Diese Möglichkeit bietet eine höhere Sicherheit vor Mißbrauch. Außerdem ist der Benutzer auch nicht mehr an einen bestimmten Apparat gebunden, sondern kann jeden anderen Apparat benutzen, da über den persönlichen Identifikationscode das Gespräch auf ihn verbucht wird. Inwieweit dies datenschutzrechtlich zulässig ist, muß in jedem Einzelfall gesondert geprüft werden.

Je größer das Funktionsspektrum eines Terminals ist, wozu heute auch der multifunktionale Nebenstellenanschluß gehört, um so mehr muß für die Sicherung vor Mißbrauch getan werden. Findet außerdem noch eine Integration mit der Datenverarbeitung beispielsweise innerhalb eines lokalen Netzes (LAN – Local area network) statt, sind Maßnahmen zur Identifikation und Authentifikation (Benutzerkennung, persönliches Kennwort, Chipkarte) unbedingt erforderlich. Jeder Benutzer darf nur auf solche Informationen und Dienste zugreifen, zu deren Kenntnisnahme, Bearbeitung und Benutzung er autorisiert wurde. Die Fernschreibdienste (Telex, Teletex und Telefax), die in ein Bürokommunikationssystem integriert sind, sind ausschließlich privilegierten Benutzern zugänglich zu machen.

Probleme bereitet in einem Inhouse-Kommunikationsnetz noch die Zugriffskontrolle. In einem sogenannten Bus-Netz (LAN) kann im Prinzip jedes angeschlossene Terminal die gesamte Kommunikation mithören. Aus diesem Grunde werden kryptographische Verfahren zunehmend an Bedeutung gewinnen. Verschlüsselte Informationen können dann zwar empfangen, aber nur von dem interpretiert werden, der den Entschlüsselungscode besitzt.

Bei der Bürokommunikation stehen wir jedoch noch ganz am Anfang. Innerhalb der Prüfungstätigkeit wurden bisher allenfalls digitale Nebenstellenanlagen angetroffen. Für die Revision wird die zunehmende Automatisierung der Büros in den nächsten Jahren aber eine weitere Herausforderung darstellen.

Die Dokumentation des Kommunikationsnetzes, seiner Teilnehmer und deren Befugnisse sowie die Protokollierung von relevanten Aktivitäten werden notwendige Hilfsmittel sein, auf denen eine Revision aufsetzen kann.

18.2. Kontrolle der technischen und organisatorischen Maßnahmen

Im Berichtszeitraum wurde die Kontrolle der technischen und organisatorischen Maßnahmen fortgesetzt. Hervorzuheben ist, daß die Zahl der Beratungen vor Ort und in meiner Geschäftsstelle weiter zunahm, so daß diese fast die Größenordnung der durchgeführten Kontrollen erreichte. Die Beratungen bezogen sich in erster Linie auf die Organisation der DV und die baulichen Gegebenheiten. Überprüft wurden die technischen und organisatorischen Maßnahmen zur Datensicherung bei 4 Großrechenzentren, 3 kreisfreien Städten, 6 kreisangehörigen Gemeinden, 3 Landratsämtern, 5 medizinischen Versorgungseinrichtungen und bei 2 Körperschaften des öffentlichen Rechts, darunter einer großen Allgemeine Ortskrankenkasse.

Die Prüfungen zeigten, daß grobe Verstöße gegen die Vorschriften des Art. 15 BayDSG nicht festzustellen waren. Trotzdem können sich scheinbar belanglose Verfehlungen, z.B. die unsachgemäße Entsorgung von Datenträgern, zu Skandalen ausweiten, wie im letzten Jahr wiederholt in der Presse zu lesen war.

Ein Mangel, der immer wieder festgestellt werden mußte, um ein weiteres Beispiel herauszugreifen, war bei der

automatisierten Datenverarbeitung nach wie vor die fehlende Revisionsfähigkeit der Unterlagen über die Maschinenbenutzung. Hier sind vor allem die Hersteller von DV-Anlagen aufgerufen, gegen diese Schwachstelle etwas zu tun. Die Möglichkeit persönliche Kennworte als Zugriffsschutz vorzusehen, ist keine ausreichende Lösung dieses Problemes.

Mit der zunehmenden Verbreitung der Personal Computer wird eine externe Kontrolle der „Individuellen Datenverarbeitung (IDV)" – siehe dazu 18.1.2 – immer schwieriger. Der Datenschutzbeauftragte kann zwar bei der Schwachstellenanalyse Hilfestellung leisten, eine Problemlösung ist jedoch oft wegen des Fehlens ausreichender technischer und personeller Kapazitäten nicht möglich. Trotzdem konnten in vielen Fällen nützliche Anregungen zur Verbesserung der Datensicherung gegeben werden.

Bei der Einführung neuer Techniken sollte man sich jedoch unbedingt Gedanken darüber machen, wie unberechtigten Zugriffen auf Datenbestände wirksam begegnet wird. Es hilft wenig, wenn man zwar um die Schwachstellen des Sicherungssystems Bescheid weiß, jedoch wenig zu deren Behebung getan hat. In manchen Fällen wurde auf die Durchführung einer Schwachstellenanalyse ganz verzichtet.

Die Konzipierung und Einführung von Datensicherungsmaßnahmen ist stets eine Angelegenheit des Anwenders. Kontrollinstitutionen dürfen nicht als Alibi herhalten, wenn sich trotz eines Kontrollbesuches hinterher Mängel zeigten, die vorher nicht erkannt oder gesehen wurden. Der Datenschutzbeauftragte verfügt zwar über ein weites Spektrum an Erfahrungswerten, er kann jedoch nicht über die Sachkenntnis eines Spezialisten verfügen, der tagein und tagaus mit ein- und demselben Spezialgebiet und einer bestimmten Systemkonfiguration beschäftigt ist. Die Datensicherung ist dazu ein viel zu komplexes Aufgabengebiet. So erfordert es nämlich ein intensives Studium und vor allem praktische Erfahrungen, um auf die Mißbrauchsmöglichkeiten und Grenzen der Kommunikationstechnik in offenen Systemen zu kommen. Experten, die sich beispielsweise mit Abwehrmaßnahmen vor dem „Hacking" (unberechtigtes Eindringen in ein DV-System) ernsthaft beschäftigt haben, wissen, daß die vielfach vertretene Meinung, die Sicherungsmaßnahmen bei offenen Systemen seien leicht zu umgehen, einer doch recht oberflächlichen Betrachtungsweise entspringt.

18.3. Technische Einzelprobleme

18.3.1. Technische und organisatorische Maßnahmen zur Einhaltung des Persönlichkeitsschutzes

In der Öffentlichen Verwaltung ist es heute fast selbstverständlich, daß Behördenfremde nicht in Bildschirminhalte Einsicht nehmen dürfen, daß personenbezogene Unterlagen unter Verschluß aufbewahrt werden und daß ausgesonderte personenbezogene Unterlagen nicht unzerkleinert (teilentsorgt) in den Müllcontainer gelangen dürfen. Vielen Behördenangehörigen ist jedoch noch nicht bewußt, daß Datensicherungsmaßnahmen schon beim täglichen Parteienverkehr erforderlich sein können. Bei der persönlichen Beratung an den Schaltern einer Krankenkasse, bei der Patientenaufnahme im Krankenhaus, beim Besuch des Sozial-, Jugend-, Melde- und Finanzamts, um nur einige Beispiele zu nennen, können sensible Informationen ausgetauscht werden, die für Mithörer oder wartende Dritte zwar interessant, jedoch nicht bestimmt sind. Im Sechsten Tätigkeitsbericht wurde unter der Textziffer 5.1.3 (Seite 79) dieses Thema angeschnitten.

Datenschutz beim Parteiverkehr

Zu diesem Thema ergeben sich aus der Prüfungs- und die Beratungstätigkeit folgende Hinweise: Auch in den Verwaltungsbereichen, in denen vertrauliche Gespräche mit Betroffenen stattfinden, gibt es noch Amtsstuben, in denen mehrere Sachbearbeiter sitzen und gleichzeitig Parteienverkehr abwickeln. In manchen Schalterhallen bilden sich zu bestimmten Zeiten und an manchen Schaltern Schlangen von Kunden, so daß Wartende mühelos die Gespräche derjenigen mithören können, die gerade vom Schalterbeamten bedient werden. Um Platz zu sparen, oder aus baulichen Gegebenheiten, wurden mitunter die Schalter so dicht aneinandergelegt, daß sogar Gespräche am benachbarten Schalter mitverfolgt werden können. Wenn diese Beispiele auch Ausnahmen bilden, sind sie für die Betroffenen gleichwohl unerfreulich. Nicht alle Behörden sind genügend sensibilisiert oder sie sehen sich außerstande, solche Zustände zu ändern. Besucher haben oft nicht den Mut, Sachbearbeiter darauf aufmerksam zu machen, daß sie sich in ihren Persönlichkeitsrechten verletzt fühlen, sie vermeiden sensible Themen anzusprechen und versuchen ihr Glück ein zweites Mal, in der Hoffnung, dann keine Mithörer mehr vorzufinden. Gerade auf dem Land, wo die Anonymität der Großstadt fehlt, können durch derartige Zustände schutzwürdige Belange stärker beeinträchtigt sein. Es gab Fälle, daß Behördenbesucher auf den mangelhaften Persönlichkeitsschutz hinwiesen und sich an den Sachbearbeiter oder direkt an den Behörden- oder Landesdatenschutzbeauftragten wandten.

Viele Behörden haben dieses Problem erkannt und versuchen durch bauliche Maßnahmen abzuhelfen. Beim Umbau einer Schalterhalle wird nicht mehr nur an die Optik, sondern auch an den Persönlichkeitsschutz gedacht. Die Schaffung eines Geräuschpegels oder der Einbau schalldämmender Bodenbeläge und Deckenelemente (z.B. Schlitze in Holzkassettendecke) sind geeignete Hilfsmittel, ein Mithören zu erschweren. Schließlich lassen sich die Bearbeiterplätze so gruppieren – etwa in geschachtelten Bereichen – und durch schallisolierende Raumteiler voneinander abschotten, daß eine Kommunikation über zwei Schalter ausgeschlossen wird. Für die Dimensionierung der Zahl der Bearbeiterplätze gibt eine Besucherzählung wertvolle Entscheidungshilfen. Im Zuge der vielfach propagierten papierarmen Verarbeitung und des Wegfalls der herkömmlichen Karteien, deren Pflege und Verwaltung einer bestimmten Sachbearbeitergruppe oblag, ist der Besucher nicht mehr auf einen vorgeschriebenen Sachbearbeiterplatz fixiert, sondern kann sich an den Sachbearbeiter wenden, der gerade frei ist, weil dieser mittels Datensichtstation den gesamten Datenbestand im direkten Zugriff hat. Die Warteschlangen an bestimmten Schaltern entfallen, womit sich auch der Kundenservice erhöht. Für den Fall, daß trotzdem alle Schalter besetzt sind, läßt sich eine von der Bearbeitungszone abgesetzte Wartezone einrichten, von der aus die Besucher an freiwerdende Sachbearbeiterplätze gesteuert werden können.

Sind Umbaumaßnahmen in der oben beschriebenen Art nicht möglich, läßt sich auch durch organisatorische Maßnahmen eine Verbesserung des Persönlichkeitsschutzes erreichen. Sachbearbeiter können verlangen, daß Wartende Abstand halten oder erst dann das Zimmer betreten, wenn der Sachbearbeiter frei ist. Die Besucher könnten außerdem darauf hingewiesen werden, daß Möglichkeiten bestehen, Gespräche mit dem Sachbearbeiter abseits der Bearbeitungszone an einem Diskretionsschalter oder in einem Einzelzimmer zu führen.

Ganz besonders ist bei Neubau- und Umbaumaßnahmen darauf zu achten, daß die Bereiche, in denen sensible Daten erhoben und bearbeitet werden, den Anforderungen des Persönlichkeitsschutzes gerecht werden. Die Einrichtung von abgeschlossenen Einzelzimmern oder von Sprechkabinen läßt sich zwar nicht überall verwirklichen, trotzdem sollte es möglich sein, Zonen oder Bedingungen zu schaffen, die das Mithören von Gesprächen besonders sensibler Art durch unbeteiligte Dritte vermeiden. Der Besucher sollte erkennen können, daß er persönliche Daten nicht in Gegenwart unbeteiligter Dritter preisgeben muß. Hierzu bedarf es manchmal noch einer stärkeren Sensibilisierung der Sachbearbeiter, die sehr viel dazu beitragen können, daß die Besucher das Gefühl bekommen, daß die gebotene Diskretion ein Anliegen der betreffenden Behörde und nicht nur ein Schlagwort ist.

Es gibt gerade im Dienstleistungsbereich viele Beispiele, die zeigen, daß sich die Wahrung des Persönlichkeitsschutzes mustergültig realisieren läßt. Bei alledem scheint mir folgender Gesichtspunkt wichtig: In dem Maße, in dem sich der Dienstleistungs-, Hilfs- und Unterstützungssektor des Staates ausweitet, wächst auch die Menge und die Sensibilität der zu erhebenden Daten. Hieraus ergibt sich ebenso ein wachsendes Bedürfnis nach Diskretion und Datenschutz. Daß erhöhte Diskretion früher nicht nötig war, ist mithin kein Argument dagegen, daß sie heute geboten ist.

18.3.2. Vernichtung und Entsorgung von Datenträgern

Immer wieder wurde in der Presse darüber berichtet, daß Datenträger, die zur Vernichtung anstehen, Unbefugten in die Hände fielen, weil sich die Organisation und die Durchführung der Entsorgung als mangelhaft erwies.

Werden bei Schreibmaschinen statt der herkömmlichen Textilfarbbänder Carbonbänder verwendet, ist auf deren sichere Entsorgung zu achten. Carbonbänder werden nämlich nur einmal verwendet, so daß der mit ihnen geschriebene Text reproduzierbar ist.

Auch wenn Privatfirmen mit der Durchführung der Entsorgung von Datenträgern beauftragt wurden, kann sich die auftraggebende öffentliche Stelle bei Pannen nicht aus der Verantwortung ziehen, da sie ja nach wie vor für die Einhaltung der technischen und organisatorischen Maßnahmen zum Datenschutz verantwortlich ist. In jedem Fall muß sich der Auftraggeber vertraglich absichern und seinen Forderungen durch Vereinbarung einer Vertragsstrafe Nachdruck verleihen (vgl. Nr. 3.4 ff VollzBekBayDSG). Eine solche vertragliche Absicherung allein genügt jedoch als zuverlässige Sicherung der technischen und organisatorischen Maßnahmen zum Datenschutz nicht.

18.3.3. Speicherkontrolle bei Online-Verfahren

Beim Betrieb von Online-Verfahren entspricht es nunmehr dem Stand der Technik, daß für die Nutzer sogenannte Benutzerprofile definiert werden. In diesen Vorgaben wird festgelegt, welche Nutzer Zugriff zu welchen Aufgaben (Transaktionen) haben. Jede einzelne Transaktion enthält wiederum implizit die Berechtigung für das Lesen, Einspeichern, Verändern oder das Löschen von Daten. Darf ein Nutzer im Datenbestand lediglich lesen, so ist ihm der Zugang zu den Transaktionen verwehrt, die den Datenbestand verändern. Das Verändern des Datenbestandes wird man nur privilegierten Nutzern gestatten. Ist ein Datum verändert oder gar gelöscht, besitzt man in den meisten Fällen keine maschinell geführte Information darüber, wer was verändert oder gelöscht hat (Ausnahme: Logdateien von Datenbanksystemen). Aus diesem Grund werden in manchen Verfahren bei Veränderungen, Einspeicherungen und Löschungen der Verursacher, der Grund und das Datum im Datensatz mitabgespeichert. Ohne Zweifel bedeutet das einen Mehraufwand. Die Transparenz und die Revisionsfähigkeit erhöht sich aber dadurch um ein beträchtliches Maß. Gerade dort erscheint ein solches Verfahren notwendig, wo die Zugriffsberechtigung nach Wegfall der herkömmlichen Karteien auf den gesamten Datenbestand ausgeweitet wurde. In der manuellen Verarbeitung bestand, organisatorisch bedingt, lediglich auf einen begrenzten Teil der Daten, nämlich den der eigenen Kartei, Zugriff.

Exakte Zugriffs- und Veränderungsregelungen sind dort nötig, wo ein integriertes Verfahren eingesetzt wird. Löschungen und Veränderungen darf nur die Abteilung einer Stelle veranlassen, die gewissermaßen „Herr der Daten" („originäres Prinzip") ist. So kann u.U. die Kämmerei einer Gemeinde auf die Einwohneradresse zugreifen und diese beispielsweise für die Bescheidversendung verwenden. Erhält diese Stelle aber Kenntnis davon, daß die Empfängeranschrift mit der im Melderegister abgespeicherten Adresse nicht mehr übereinstimmt, darf sie keinesfalls die Einwohneradresse verändern. Für derartige Fälle sehen diese Verfahren die Abspeicherung einer eigenen Versandadresse des Bescheidempfängers in der sogenannten Finanzadreßdatei vor.

18.3.4. Die Chip-Karte

In vielen automatisierten Verfahren wird es heute als Schwachstelle angesehen, daß sich geschlossene Systeme gegen unberechtigte Eingriffe oft nur unzureichend schützen können. Zusätzliche Sicherheit beim Zugang zu einem geschlossenen Kommunikationsnetz, zu einem Anwendungssystem oder auch nur zu einem Gebäudeteil, in dem sich ein besonders sensibler Bereich befindet, bietet die Chip-Kar te, mit der als persönlicher Identifikationsausweis die Identität einer Person – ähnlich der Unterschriftsprobe im Zahlungsverkehr – festgestellt werden kann.

Die Chip- oder Memory-Karte enthält einen „intelligenten Chip". Dieser Chip hat zwei Eigenschaften: Einmal enthält der Chip einen dreiteiligen Speicher, in dem ein nicht veränderbarer Geheim-Code und ein geschützter Code, der nur dem Karteninhaber zugänglich gemacht werden kann, gespeichert sind, der Rest ist für die Speicherung von freizugänglichen Daten vorgesehen. Darüber hinaus enthält

der Chip einen Mikroprozessor, der selbständig Daten verarbeiten kann. Auf diese Weise läßt sich die nicht allgemein zugängliche Information vor unberechtigten Zugriffen schützen. Mit dem Mikroprogramm können auch Rechenoperationen durchgeführt werden. Von dieser Eigenschaft wird vor allem im kommerziellen Zahlungsverkehr dergestalt Gebrauch gemacht, daß auf der Karte der aktuelle Kontostand des Inhabers gespeichert ist und bei Zahlungen um den jeweiligen Betrag reduziert wird, so daß die Karte stets die augenblickliche Zahlungsfähigkeit des Besitzers ausweist. Damit eine Abbuchung nicht von jedem X-Beliebigen vorgenommen werden kann, muß sich der Besitzer durch einen persönlichen Identifikations-Code, der am Lesegerät eingetastet wird, ausweisen. Dieser persönliche Identifikations-Code wird von einem Mikroprogramm in einen geheimen Schlüssel umgewandelt. Stimmt dieser Schlüssel mit dem auf der Karte gespeicherten Geheim-Code überein, gilt die Identität der berechtigten Person als festgestellt. Auf diese Weise kann sich der Eigentümer der Chip-Karte gegen mißbräuchliche Benutzung durch Fremde ausreichend sichern.

Dieses Verfahren wird auch oft als Schlüssel zu besonders sensiblen Bereichen verwendet, wie z.B. zum inneren Sicherheitsbereich eines Rechenzentrums, zum Zugang zu einem Terminal oder zum Zugang zu einer bestimmten Anwendung, in der sensible Datenbestände verarbeitet werden. Bei wiederholter mißbräuchlicher Anwendung der Chip-Karte (z.B. das persönliche Kennwort im „Trial and Error-Verfahren" herauszubekommen) kann diese von den Lesegeräten eingezogen werden.

Auch in der Datenverarbeitung macht man von der Verschlüsselung der persönlichen Kennwörter zunehmenden Gebrauch. Die persönlichen Kennwörter werden über einen bestimmten, meist auch allgemein bekannten Algorithmus verschlüsselt abgespeichert. Der Schlüsseltext enthält keine Hinweise auf die ursprüngliche Information. Weist sich nun ein Benutzer durch sein persönliches Kennwort aus, so wird dieses Kennwort vom Schlüsselprogramm in einen entsprechenden Schlüsseltext umgesetzt. Stimmt dieser Schlüsseltext mit dem gespeicherten überein, gilt der Benutzer als zugriffsberechtigt. Zu beachten ist, daß man mit der Eingabe des verschlüsselten Kennwortes keinen Zugriff auf die durch dieses Kennwort geschützten Informationen erhält. Deshalb ist es nicht notwendig, die Datei der persönlichen Kennworte besonders zu schützen, da die Ursprungsinformation irreversibel chiffriert ist. Dieses Verfahren wird Einwegverschlüsselung genannt.

18.3.5. Fernwartung von DV-Systemen

Die Bedeutung der Fernwartung von DV-Systemen nimmt ständig zu. Während es noch vor zehn Jahren üblich war, daß ein Wartungstechniker lediglich für die Wartung einer DV-Anlage zuständig war und seinen Arbeitsplatz unmittelbar im Rechenzentrum hatte, trifft diese Aussage nur noch für ganz wenige, besonders große Installationen zu. Die Vielzahl der dezentralen DV-Systeme, die Stabilität der Hardware, die Komplexität der Komponenten und die gestiegenen Personalkosten waren die Ursachen dafür, daß die Hersteller – auch im Kundeninteresse einer effektiven Betreuung und der Kostenersparnis (Zentralisierung des Wissens) – die Fernwartung einführten.

Um Fernwartung durchführen zu können, benötigt man heute einen Leitungsanschluß, der meist aus einem Akustikkoppler besteht und ein Telefon. Vom Fernsprechapparat wird die Fernwartungszentrale angerufen und sobald die Datenleitung steht, wird der Hörer in den Akustikkoppler gelegt. Das dezentrale DV-System ist dann über eine Wählleitung mit der Wartungszentrale verbunden.

Um den Anwendern, die mit der Technik weniger vertraut sind, eine Orientierungshilfe über die Art der Maßnahmen zur technischen Absicherung der Fernwartung zu geben, wurde in Zusammenarbeit mit dem Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder ein Fragenkatalog zusammengestellt. Maßnahmen, die der Betreiber eines DV-Systemes zu treffen hat, sind als Anlage dem Bericht beigefügt. Maßnahmen, die vom Hersteller zu erbringen sind, wurden aus Gründen der Lesbarkeit ausgeklammert, da diese systemabhängig sind und deshalb unterschiedlich ausfallen. Mit den Herstellern abgestimmte Auswertungen gibt es für die Systeme Hewlett-Packard 3000/XX, IBM 43XX, 303X/3081, Kienzle 90XX (MTOS), NCR Serie 9000, Nixdorf 8860/8870, Siemens BS 2000/3000. Sie liegen in meiner Geschäftsstelle auf.

Ein Wählleitungsanschluß an einem DV-System wird heute immer wieder als Schwachstelle angesehen, weil über diese Verbindung Unberechtigte (z.B. „Hacker") Zugriff auf Programme und Daten erhalten können. Verfügt ein DV-System jedoch lediglich über einen Akustikkoppler, ist ein Einwählen von außen ohne Mitwirkung des Systembedieners nicht möglich. Aber auch bei Wählleitungsanschlüssen gibt es eine Reihe von softwaretechnischen Möglichkeiten, Eindringlinge als solche zu erkennen und abzuweisen.

Für die Fernwartung sollte allerdings stets gelten, daß der Verbindungsaufbau zur Fernwartungszentrale vom Kunden aus erfolgt, so daß ein automatisches Einwählen ohnehin nicht vorgesehen ist. Damit vom DV-System keine Verbindung zu einem anderen als der Fernwartungszentrale hergestellt werden kann, gibt es für den Fernsprechanschluß Zusatzgeräte, in die die Teilnehmernummer der Fernwartungszentrale eingespeichert wird, so daß ausschließlich diese Teilnehmernummer angerufen werden kann. Das Zusatzgerät ist abschließbar, so daß Manipulationen weitgehend ausgeschlossen sind bzw. im Nachhinein erkannt werden.

Stammt auch die Anwendungssoftware vom Hersteller, kann eine Fehleranalyse und -behebung in der Regel nur unter Berücksichtigung der betroffenen Datenbestände erfolgen. Daß die Anwender wegen einer eventuell damit verbundenen Offenbarung von personenbezogenen Daten an den Hersteller auf die Fehlerbehebung verzichten, wird man gerade von Anwendern dedizierter Systeme, die ohnehin wenig Systemkenntnisse besitzen, nicht erwarten können. In solchen Fällen ist der Anwender gehalten, sich gegen Mißbrauch im Sinne Nr. 3.3 VollzBekBayDSG vom 12.9.1978 (MABl 27/1978) vertraglich abzusichern.

18.3.6. Mikroverfilmung von Schriftgut

Die Verfilmung von Schriftgut ist heute eine beliebte Art, das Mengenproblem archivierter Unterlagen (Passivverfilmung) zu bewältigen. Entschließt sich eine Behörde für den

Mikrofilm/Mikrofiche als Speichermedien, hat sie zu prüfen, ob sie die Schriftgutverfilmung selbst erledigt, oder an einen Auftragnehmer vergibt. In beiden Fällen ist auf die notwendigen Datensicherungsmaßnahmen zu achten. Besondere Datensicherungsprobleme können bei der Außerhausverfilmung auftreten.

Dabei ist zu prüfen, ob es die Sensibilität des Datenmaterials zuläßt, daß dieses außer Haus gehen kann und somit Dritten offenbart wird, auch wenn der Auftragnehmer den Inhalt des Schriftgutes tatsächlich nicht zur Kenntnis nimmt.

Analog dem Schutzstufenkonzept bei der Verarbeitung personenbezogener Daten auf Großrechnern erscheint es auch bei der Mikroverfilmung zweckmäßig, die zu verfilmenden Daten nach ihrer Sensibilität zu gruppieren, um die dem Schutzzweck angemessene Organisation zu finden.

Denkbar wäre folgende Klassifizierung:
Stufe 1: Daten ohne besondere Sensibilität
Stufe 2: Sensible Daten
Stufe 3: Daten, die einem außergewöhnlichen Geheimnisschutz unterliegen (z.B. Patientendaten, soweit sie Diagnosen enthalten).

Bei der Verfilmung ist grundsätzlich die Einhaltung der Normen (DIN 19053 und 19059) sowie weiterer zum Stand der Technik gehörender Standards zu beachten.

Als Orientierungshilfe für die Entscheidung Eigen- oder Außerhausverfilmung könnte folgender Vorschlag dienen:

1) Daten ohne besondere Sensibilität:
Die Verfilmung Voraussetzung außer Haus von Privatunternehmen erledigt werden, daß ausreichende vertragliche Regelungen über Art und Umfang der Sicherungsmaßnahmen bestehen.

2) Sensible Daten:
Verfilmung und Filmprüfung ist außer Haus möglich, wobei die Nebenarbeiten der Auftraggeber erledigen sollte. Bei Auftragsvergabe sind wiederum vertragliche Regelungen über die Sicherungsmaßnahmen vorzusehen.

3) Daten, die einem außergewöhnlichen Geheimnisschutz unterliegen:
In diesem Falle sollte von der Auftragsvergabe an Privatunternehmen abgesehen werden. Die Verfilmung einschließlich aller Nebenarbeiten sollte durch die speichernde oder eine andere öffentliche Stelle erledigt werden, sofern nicht zwingende wirtschaftliche Überlegungen dagegenstehen.

Daneben sind eventuelle rechtliche Hindernisse einer Auftragsvergabe an Dritte zu beachten: Regelmäßig muß hier geprüft werden, ob eine „befugte" Offenbarung an den Auftragnehmer vorliegt (siehe z.B. § 203 StGB, § 30 AO, § 76 SGB X).

Dem Anhang wurde eine Zusammenstellung beigefügt, aus der alle bei der Schriftgutverfilmung notwendigen Arbeitsschritte, deren Risiken sowie die Maßnahmen zur Risikoverminderung zu entnehmen sind.

18.3.7. Kryptographie

In den letzten Jahren, insbesondere seit Bestehen der Datenschutzaufsichtsinstanzen, hat die Datenfernverarbeitung stetig zugenommen: Immer mehr Daten werden über Leitungen geschickt, sei es über festgeschaltete Leitungen oder Wählleitungen; vielfach werden Daten über Richtfunkstrecken übertragen. Auch die Übertragungsgeschwindigkeit ist höher geworden, so daß größere Datenmengen wirtschaftlich übertragen werden können. Für Leute, die es darauf anlegen, Datenverkehr abzuhören, tut sich eine ergiebige Informationsquelle auf. Zwar sind viele Daten aus sich heraus nicht verständlich, doch ist nicht auszuschließen, daß derjenige, der abhört, über genügend Sachkunde verfügt und sich zur Auswertung und Zusammenführung der Datenfragmente ebenfalls der elektronischen Datenverarbeitung bedient. So gesehen wird der Ruf nach einer sicheren und billigen Verschlüsselung der Daten, bevor diese in Leitungen übertragen werden, immer lauter.

Nachdem auch die DV-Hardwarekosten immer niedriger wurden, und die Verarbeitungsgeschwindigkeit ständig gestiegen ist, können heute Verschlüsselungsmethoden durchaus wirtschaftlich betrieben werden. In der Vergangenheit scheiterte eine Verschlüsselung häufig noch am Verarbeitungsaufwand. Billige und einfache Verschlüsselungstechniken, wie zum Beispiel Codesysteme, bieten gegen einen fachkundigen Abhörenden heute nur einen geringen Schutz, so daß ihr Einsatz nur begrenzten Wert hat.

Neben den Codesystemen kennt die Kryptographie noch die sogenannten Kryptosysteme: Bei den Kryptosystemen unterscheidet man reversible Chiffren und irreversible Chiffren. Bei den reversiblen Chiffren gibt es kontinuierliche Chiffren und Blockchiffren, wozu der DES-Algorithmus (data encryption standard) gehört. Zu den irreversiblen Chiffren gehören die Systeme mit offenen Schlüsseln (z.B. das RSA-Verfahren, siehe unten).

In der Praxis wird heute in erster Linie mit reversiblen Chiffren gearbeitet. Bei den reversiblen Chiffren dient der Verschlüsselungsschlüssel auch zum Entschlüsseln des Schlüsseltextes, so daß er geheimgehalten werden muß. Manche Hersteller bieten eine Softwarelösung an, andere packen den Schlüssel in die Hardware eines Verschlüsselungsgerätes. Die Softwarelösung ist meist etwas billiger, als die Hardwarelösung, die jedoch zusätzliche Sicherheiten gegen ein Ausspähen der Schlüssel durch den Insider bringt (Hardwareschutz ist sicherer als Softwareschutz). Grundprinzip bei allen Spielarten sollte jedoch sein, daß der Schlüssel nicht mit der Nachricht übertragen wird. Da bei der Übertragung Fehler auftreten können, arbeiten solche Verschlüsselungstechniken problemloser, bei denen der Text auch dann entschlüsselt werden kann, wenn ein oder mehrere Bits verfälscht wurden. Schließlich wurden diese Algorithmen so verfeinert, daß gleiche Texte zu unterschiedlichen Zeiten verschlüsselt, unterschiedliche Schlüsseltexte ergeben. Auf diese Weise geht die Zahl der Versuche, den Text durch Probieren zu entschlüsseln, praktisch ins Unendliche. Die Verschlüsselung ist dadurch im Ergebnis zuverlässig.

Bei irreversiblen Chiffren, den Public-Key-Systemen, wird mit einem sogenannten öffentlichen Schlüssel verschlüsselt und mit einem geheimen Schlüssel entschlüsselt. Nach den Erfindern des Public-Key-Systems Rivest, Shamir und Adleman wird das Verfahren auch als RSA-Verfahren

bezeichnet. Es soll mathematisch gesehen noch sicherer als die Verfahren mit reversiblen Chiffren sein. Unklarheit herrscht allerdings noch darüber, wer oder welche Stelle die öffentlichen und vor allem die geheimen Schlüssel verwalten soll. Eine derartige Stelle hätte dann theoretisch Zugang zu allen geheimen Informationen.

18.4. Datensicherung bei den Neuen Medien

Die Technik der Neuen Medien ist besonders gründlich zu untersuchen. Nur derjenige, der die technischen Einzelheiten zuverlässig kennt, kann wirkungsvolle Datensicherungsmaßnahmen vorschlagen und so zur Verbesserung der Systeme beitragen.

18.4.1. Datensicherungsmaßnahmen bei Bildschirmtext

Bildschirmtext gilt als offenes System zur Nutzung durch jedermann. Mit Bildschirmtext können, wie bereits in früheren Tätigkeitsberichten dargelegt, Informationsseiten abgerufen, Mitteilungen an andere Teilnehmer versandt und der Zugang zu externen Rechnern ermöglicht werden. Zwar ist eine hundertprozentige technische Sicherheit dieses für jedermann zugänglichen, offenen Systems mit wirtschaftlich betriebenen Aufwand nicht möglich, wegen des Umfangs und der angestrebten Verbreitung dieses Systems sind jedoch besondere Anforderungen an die Sicherungsmaßnahmen zu stellen. Nicht zuletzt können durch Mängel im Sicherungskonzept dem Teilnehmer und vor allem aber dem Anbieter finanzielle Nachteile erwachsen.

Sicherungsmaßnahmen

Bei Bildschirmtext sind folgende Sicherungsmaßnahmen verwirklicht:

- Der Verbindungsaufbau geschieht in der Regel durch eine geheime Anschlußkennung, die von der Anschlußbox ausgesandt wird. Bei Verwendung eines Datenmodems muß diese Anschlußkennung von Hand eingegeben werden. Die Anschlußkennung ist zwölfstellig, bundesweit eindeutig und setzt sich ausschließlich aus Ziffern zusammen. Das System unterscheidet zwischen Anschlußkennungen der Anschlußbox und solchen, die Datenmodems zugeordnet werden. Die Anschlußbox hat eine halbe Sekunde Zeit, die Anschlußkennung abzusenden. Geschieht das nicht innerhalb dieser Zeit, wird die Verbindung gelöst. Dies bedeutet einen erheblichen Schutz gegen Mißbrauch.
- Der Zugang zu Bildschirmtext ist zudem nur über die Eingabe eines persönlichen Kennwortes möglich. Die Anmeldung beim System erfolgt demnach über ein zweistufes Identifikationsverfahren. Trivial aufgebaute persönliche Kennwörter werden vom System abgewiesen. Die persönlichen Kennworte können den gesamten Zeichenvorrat umfassen.
- Im allgemeinen ist jedem Teilnehmer ein Anschluß fest zugeordnet. Das bedeutet, daß von einer ganz bestimmten Anschlußbox nur ein bei der Einrichtung des Anschlusses definierter Teilnehmer aktiv werden kann. Innerhalb der Systemvariablen reicht die Deutsche Bundespost die Teilnehmernummer zur Identifizierung des Teilnehmers an den externen Rechner weiter. Das funktioniert dann nicht mehr, wenn die feste Zuordnung aufgehoben ist und Teilnehmer und Anschluß freizügig geschaltet sind. Ein freizügiger Teilnehmer kann nur an einem freizügigen Anschluß arbeiten.
- Beim home-banking muß der Teilnehmer neben seiner Kontonummer auch die geheime persönliche Identifikationsnummer (PIN) und bei Bankgeschäften eine sogenannte Transaktionsnummer (TAN) dem Rechner mitteilen. Über eine Transaktionsnummer ist jeweils nur ein Bankgeschäft durchführbar. Die PIN und die TAN's werden dem Teilnehmer vom Bankinstitut bei Beachtung bestimmter Sicherheitsvorkehrungen (verdeckter Ausdruck, getrennte Zustellung) zugeteilt.
- Nach mehreren unmittelbar aufeinander folgenden Fehlversuchen bei der Eingabe des persönlichen Kennworts und der PIN ergreifen sowohl das Btx-System der DBP als das Anwendungssystem des betreffenden Geldinstituts von sich aus Maßnahmen, in dem entweder der Anschluß gesperrt oder der Teilnehmer von weiteren Ausforschungsversuchen ausgeschlossen wird.
- Mitteilungen und Mailboxen werden in gleicher Weise geschützt.
- Die Zusammenfassung bestimmter Teilnehmer zu einer geschlossenen Benutzergruppe kann eine weitere Sicherheit bedeuten. Anbieter können auf die Weise anderen Teilnehmern, die nicht der geschlossenen Benutzergruppe angehören, den Zugang zu Bildschirmseiten verwehren.

Technische Risiken und Möglichkeiten, ihnen zu begegnen

Da Bildschirmtext ein offenes System ist, sind an die Geheimhaltung der Anschluß-/Benutzerkennungen und der persönlichen Kennworte hohe Ansprüche zu stellen. Als Risiken sind deshalb die unverschlüsselte Speicherung der persönlichen Kennworte in der Bildschirmtext-Zentrale und vor allem die unverschlüsselte Übertragung von Kennwörtern über die Fernsprechleitungen anzusehen. Die Übertragung der Information vom Endbenutzer zur Bildschirmtextvermittlungsstelle erfolgt nämlich im Fernsprechnetz. Das Fernsprechnetz bietet bekanntlich keine absolute Abhörsicherheit. Mit Hilfe von Personalcomputern ist es möglich, den Datentransfer aufzuzeichnen und somit die Kennungen und die persönlichen Kennworte unter Umständen in Erfahrung zu bringen. Besteht Teilnehmerfreizügigkeit, kann mit einem solchen Kennwort Bildschirmtext zu Lasten eines anderen genutzt werden. Die Deutsche Bundespost plant hier Abhilfe dadurch zu schaffen, daß es nicht mehr möglich sein soll, von freizügigen Anschlüssen gebührenpflichtige Seiten abzurufen. Außerdem soll die Höhe der Vergütungen für den Aufruf von entgeltpflichtigen Seiten einer Sitzung begrenzt werden.

Mit der Einführung einer Chipkarte, auf der die Identifikationskennung verschlüsselt abgespeichert ist, möchte die Bundespost ab 1986 verhindern, daß unter falscher Teilnehmernummer eine Verbindung simuliert werden kann. Mit dieser Maßnahme ließe sich ein hoher Grad an Sicherheit erreichen.

Schließlich können bestimmte Sicherheitsvorkehrungen bei vorsätzlichem Mißbrauch umgangen werden, wie z.B. die Sperrung eines Anschlusses nach mehreren falschen Eingaben des persönlichen Kennwortes. Eine zusätzliche

Sicherheit würde es bedeuten, wenn der Teilnehmer über die Fehlversuche unter seiner Anschlußkennung unterrichtet würde, so daß er Ausforschungsversuchen durch Änderung seines Kennwortes begegnen könnte.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder hat nach zahlreichen Gesprächen mit Vertretern der DBP eine Btx-Verfahrensbeschreibung (1. Ausbaustufe, Stand 17.1.1985) erstellt. Sie ist ein gutes Hilfsmittel zur Bewertung der Risiken, zumal sie auch eine Risikoanalyse und Vorschläge zur Verbesserung der Datensicherung aus der Sicht des Arbeitskreises enthält. Die Verfahrensbeschreibung ist mit der DBP abgestimmt.

18.4.2. TEMEX, ein Datei-Dienst der Deutschen Bundespost

Die Deutsche Bundespost hat – wie bereits oben erwähnt – mit Piloteinsatz einen neuen Datenübertragungsdienst, den sog. TEMEX-Dienst (Telemetry Exchange) begonnen.

Dabei umfaßt Fernwirken das Fernüberwachen und Fernsteuern räumlich entfernter Objekte (Endeinrichtungen) von unterschiedlichen Orten (Zentralen) aus. Der Datenfluß erfolgt beim Fernüberwachen von den Endeinrichtungen in Richtung Zentrale, wobei die Anforderung, Daten auszusenden, von der Zentrale kommt und beim Fernsteuern in umgekehrter Richtung. Das Fernüberwachen umfaßt das Fernmessen (z. B. Ablesen von Zählerständen) und das Fernanzeigen (z.B. Alarmübertragung bei Notsituationen), das Fernsteuern, das Ferneinstellen (z.B. Lenkung von Energie, Steuerung von Ampelanlagen) und das Fernschalten (z.B. Beleuchtung, Alarmanlage). Die Fernwirkverbindung kann über eine festgeschaltete Leitung (HfD = Hauptanschluß für Direktruf) oder über eine Wählleitung hergestellt werden.

Während bei der Fernanzeige und beim Fernschalten nur Signale übertragen werden, sollen bei der Fernmessung digitale Werte auf den Leitungen von Endbenutzer über die TEMEX-Vermittlungsstelle zur Zentrale (Anbieter) fließen. Bei der Ferneinstellung handelt es sich im wesentlichen um die Steuerung von Prozessen, die letztlich wieder durch den Austausch von Signalen erfolgt. Die TEMEX-Vermittlungsstelle dabei muß erkennen können, von wem eine Information stammt und an wen sie weitergeleitet werden soll. Sie muß den Absender dem Empfänger zuordnen können.

Bei der Übermittlung von Fernwirk-Informationen von einem Endbenutzeranschluß zum zugehörigen Anbieteranschluß unterscheidet man 3 unterschiedliche Techniken:

- Im Bedarfsfalle werden zweiwertige Informationen, wie sie für die Übertragung einer Alarmmeldung im Regelfall ausreichen, über die Fernsprechleitung übermittelt. Dabei wird die Endeinrichtung innerhalb einer Zykluszeit von ca. 3 sec regelmäßig abgefragt, ein eventuell stehender Alarm erkannt und an die Zentrale weitergegeben.
- Zur Differenzierung und näheren Lokalisierung eines Alarms reicht eine zweiwertige Information jedoch nicht aus, weshalb die 2. Stufe die Übertragung von 8 Bits zu denselben Zeitbedingungen wie in Stufe 1 vorsieht. In dieser Technik lassen sich auch einfache Meßwerte (0-255) darstellen.
- Für Fernwirkanwendungen, die weniger zeitkritisch sind, existiert die Möglichkeit des Transports größerer Informationsmengen, nämlich 3 „Wörter" mit insgesamt 12 Bitgruppen zu je 8 Bits (Byte), wie sie für die Darstellung von Zählerständen notwendig sind. Mit einem TEMEX-Netzanschluß sollen standardmäßig zwei Datenübertragungen im Monat möglich sein.

Je Gebäude ist eine Anschlußleitung vorgesehen. Das sog. TEMEX-Netz setzt sich aus Teilnetzen zusammen, da die Daten wegen der engen regionalen Zuständigkeiten der Anbieter nur über geringe Entfernungen übertragen werden müssen. Während die Alarmmeldungen vom Nutzer und die Signale zur Fernsteuerung (zeitkritische Informationen) **unmittelbar** an die Zentrale weitergeleitet werden, kann es vorkommen, daß im Rahmen der Fernmessung, die nicht zeitkritisch ist, bei der DBP, beispielsweise in einer TEMEX-Vermittlungsstelle, eine Zwischenspeicherung der Daten erfolgt. Die Daten sollen blockweise an den jeweiligen Empfänger gesandt werden. Die Dauer der Zwischenspeicherung soll 3 bis 4 Tage nicht überschreiten.

19. Datenschutzregister

19.1. Stand

Die Zahl der eingegangenen Meldungen ist im Berichtszeitraum gegenüber dem Vorjahr leicht angestiegen. Die im Bayerischen Staatsanzeiger veröffentlichte Übersicht über den Inhalt des Datenschutzregisters mußte wegen ihres Umfangs in 2 Teilen (Nr. 49/1984 und Nr. 50/1984) erscheinen und enthält Angaben von insgesamt 4.125 speichernden Stellen mit ca. 14.200 automatisierten Dateien mit personenbezogenen Daten, das bedeutet bei den Dateien eine Zunahme von 1000 Anmeldungen. Redaktionsschluß war der 23. Oktober 1984. Die Veröffentlichung bewirkte, daß viele speichernde Stellen, vor allem aus dem Kommunalbereich, an ihre Meldepflicht erinnert wurden. Die Zahl der Rückfragen, Neueingänge und Änderungsmeldungen stieg erstmalig nach Erscheinen der Übersicht sprunghaft an. Hinzu kommt, daß die Automation weiter fortschreitet und ein Trend zu dezentralen, autonomen DV-Systemen erkennbar ist.

Die Übersicht über das Datenschutzregister ist in meiner Geschäftsstelle auf einem Textautomaten gespeichert, was die Pflege sehr erleichtert und mit dem vorhandenen Personal die Führung der Übersicht in der bekannten Form überhaupt erst ermöglicht. Damit bin ich in der Lage, jedem Bürger bezugnehmend auf seinen Wohnsitz ohne Zeitprobleme eine aktuelle Aufstellung der Behörden anfertigen zu lassen, die Daten über ihn gespeichert haben könnten. Er ist also nicht gezwungen in der gesamten Übersicht, die ohnehin nur bei Erscheinen den Stand zum Stichtag (1984 war es der 23.10.) wiedergibt, die für ihn zuständigen Behörden selbst herauszusuchen. Die Kosten für die Veröffentlichung der Übersicht sind jedoch beträchtlich. Zwar werden die auf dem Textautomaten gespeicherten Informationen auf einen maschinell lesbaren Datenträger übernommen, der als Eingabe für die Druckvorlage dient, wodurch die hohen Setzkosten entfallen. Für die von mir angeforderten Überstücke, die ich zur Verteilung an Interessenten benötige, mußte ich immerhin noch etwa 2,-

DM je Heft bezahlen. Bei dem Ausgabemedium Mikrofiche ließen sich die Kosten auf gut ein Zehntel reduzieren. Den Inhalt der 324 Seiten (Teil I und Teil II) ließe sich bequem im COM-Verfahren (Computer-Output on Mikrofilm) auf zwei Mikrofiche bringen. Für den Bürger wäre eine Mikrofilmausgabe allerdings kaum nutzbar.

Welche Entwicklung das Datenschutzregister nimmt, kann ich heute nicht beurteilen. Zu vermuten ist, daß die Pflege dieses Registers noch lange die Arbeitszeit einer Dienstkraft beanspruchen wird. Die Verfahren ändern sich, was nahezu immer mit einer Änderungen der Meldungen zum Datenschutzregister verbunden ist. Zur Zeit wird an der maschinellen Erschließung des Inhalts des Registers gearbeitet.

Die Zahl der Bürgeranfragen an das Datenschutzregister blieb gegenüber dem Vorjahr in etwa konstant. Das Interesse der Bürger, vor allem in den Ballungszentren München, Augsburg und Nürnberg ist nach wie vor groß, wenngleich immer noch falsche Vorstellungen über den Inhalt des Registers bestehen.

19.2. Vollständigkeit des Datenschutzregisters und „Bagatell"-Dateien

Aus Anlaß der Freigabe gem. Art. 26 Abs. 2 BayDSG für eine automatisiert geführte Datei, die nur wenige Angaben über Benutzer einer Bücherei enthält, wurde die Frage aufgeworfen, ob es sich lohne, solche Dateien in das Datenschutzregister einzustellen. Ich habe dazu die folgende Ansicht vertreten:

Das Bayerische Datenschutzgesetz sieht vor, daß das Datenschutzregister einen Überblick über alle automatisierten Dateien öffentlicher Stellen mit personenbezogenen Daten gibt. Die Aufgabe des Registers besteht nun nicht nur darin, Informationen über die einzelnen in das Register aufgenommenen Dateien bereitzuhalten, sondern auch in der Schaffung einer vollständigen Übersicht über die Automation in der öffentlichen Verwaltung Bayerns. Für Bagatellfälle sieht das Gesetz keine Ausnahme vor.

Erst die Vollständigkeit des Datenschutzregisters ergibt für Betroffene und für die Öffentlichkeit den Nachweis über den jeweils erreichten Grad der Automatisierung in der Verwaltung. Daraus lassen sich ggf. Anhaltspunkte für Probleme gewinnen, die aus fortschreitender Automatisierung resultieren können. Umgekehrt kann sich aus dem Register jedoch auch der beruhigende Hinweis auf die Harmlosigkeit der Automatisierung eines bestimmten Bereichs ergeben.

Auch wenn kleinere Dateien mit unsensiblen Daten für sich gesehen mehr eine Belastung als eine Bereichung des Registers darstellen, ergibt die Beschreibung dieser kleinen Dateien im Register zusammen mit dem Gesamtüberblick über die übrigen gespeicherten Daten ein konkretes Bild darüber, ob sich aus der automatisierten Datenverarbeitung Beeinträchtigungen oder problematische Tendenzen ergeben. Bei dem Fall, der zu diesen Überlegungen veranlaßt hatte, handelte es sich im weitesten Sinne um Personaldaten. Bei Personaldaten besteht ein besonderes Interesse der Betroffenen, Überblick über alle in automatisierten Verfahren gespeicherte Angaben erlangen zu können. Die Ausgestaltung der einzelnen Dateien gibt dabei Anhaltspunkte zur Klärung der Frage, ob Nutzungsmöglichkeiten bestehen, die Belastungen erwarten lassen. Sind solche nicht zu erwarten – um so besser! Ich meine, daß auch eine solche Information aus dem Datenschutzregister sinnvoll ist.

Ich halte es daher für grundsätzlich erforderlich, alle automatisierten Speicherungen personenbezogener Daten in der bayerischen öffentlichen Verwaltung in das Datenschutzregister einzustellen.

20. Bankauskunftsverfahren und Schufa

Wie in der Presse berichtet, hatten sich auch die Datenschutzbeauftragten mit den Voraussetzungen und Grenzen des Bankauskunftsverfahrens befaßt. Daneben wurde auch über die Notwendigkeit gesprochen, die sog. Schufa-Klausel zu überarbeiten und die Anforderungen des Bundesverfassungsgerichts zu berücksichtigen. Ziel der Verhandlungen war, die Kunden über den Inhalt und den Zweck des Verfahrens umfassend zu unterrichten und sie auf ihre Rechte hinzweisen. Die erzielte Einigung ist in einem Kommunique festgehalten das diesem Tätigkeitsbericht als Anhang beigefügt ist.

Der Bundesgerichtshof hat in einem Urteil vom 19.9.1985 die bisherige Schufa-Klausel für nach § 9 AGBG unwirksam erklärt und damit die entsprechenden Bedenken der Datenschutzbeauftragten bestätigt.

21. Datenschutz beim Bayerischen Rundfunk

Nach Art. 21 Abs. 3 BayDSG wird die Einhaltung des Datenschutzes im Bayerischen Rundfunk vom dortigen Datenschutzbeauftragten überwacht, der jährlich über seine Tätigkeit einen Bericht erstattet. Dem Bericht des Datenschutzbeauftragten des Bayerischen Rundfunks für den Zeitraum vom 1.1.1984 bis 31.12.1984 lassen sich folgende Schwerpunkte entnehmen:

Im Bereich der Hauptabteilung Honorare und Lizenzen hatte es, wie bereits im letzten Tätigkeitsbericht angesprochen, Probleme bei der Übermittlung von Hononardaten festangestellter Mitarbeiter anderer Rundfunkanstalten an deren Heimatanstalten gegeben. Der Datenschutzbeauftragte teilt hierzu mit, daß diese Probleme mittlerweile gelöst worden seien. Sämtliche Betroffenen seien darüber informiert worden, daß ihre Honorardaten an die Heimatanstalt übermittelt werden.

Im Personalbereich des Bayerischen Rundfunks standen die Erfahrungen mit dem 1983 eingeführten Personaldatensystem (PDS), die Vorbereitungen für ein neues Gehaltsabrechnungssystem sowie Fragen der Telefondatenerfassung im Vordergrund der Tätigkeit des Datenschutzbeauftragten. Durch die auf Vorschlag des Datenschutzbeauftragten vorgenommene Information aller Mitarbeiter über die im PDS gespeicherten Daten sei die Akzeptanz von PDS durch die Mitarbeiter voll erreicht worden. Hinweise von Mitarbeitern auf vereinzelte falsch gespeicherte Daten hätten zur Berichtigung dieser Daten im PDS geführt. Bei der Telefondatenerfassung stand die bisher durch die Rechtsprechung noch nicht abschließend geklärte Frage

zur Diskussion, ob auch die Privatgespräche der Mitarbeiter erfaßt und nach ihren äußeren Merkmalen registriert werden dürfen. Der Datenschutzbeauftragte hat insoweit eine Anonymisierung der angerufenen Telefonnummern gefordert, z.B. dadurch, daß die letzten zwei oder drei Stellen der Telefonnummern nicht gespeichert werden. Entsprechende Maßnahmen zur Umsetzung dieser datenschutzrechtlichen Anforderung seien bereits in Angriff genommen.

Der Datenschutzbeauftragte berichtet ferner über das bei allen Landesrundfunkanstalten in Planung befindliche Projekt „EDV-Einsatz im Fernsehprogrammpool". Danach sollen Daten wie Autor, Redakteur, Regisseur, Titel und Inhalt von Fernsehprogrammen, die von einer Rundfunkanstalt erworben oder produziert wurden, künftig auf Datenbänder im Umlaufverfahren allen Landesrundfunkanstalten zugeleitet werden. Die Frage, ob auf diese Übermittlung publizistischer Daten zwischen den einzelnen Landesrundfunkanstalten das Medienprivilig (Art. 21 Abs. 4 BayDSG) anwendbar ist, hat der Arbeitskreis „Rundfunkdatenschutzbeauftragte" nach eingehender Diskussion bejaht. Der Datenschutzbeauftragte des Bayerischen Rundfunks hat daher gegen das Projekt keine Einwendungen erhoben.

Einen breiten Raum im Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten nimmt wiederum der Themenbereich „Datenschutz bei der GEZ" ein. Die GEZ führt für die Rundfunkanstalten und das Zweite Deutsche Fernsehen den Gebühreneinzug durch; sie bearbeitet auch einfache Anfragen und sonstigen Routineschriftwechsel von Rundfunkteilnehmern in Datenschutzangelegenheiten. Der Rundfunkgebühreneinzug war im Berichtszeitraum Gegenstand kritischer Berichterstattung in den Medien. So waren etwa die Vorgehensweisen der GEZ zur Aktualisierung ihres Adreßbestandes sowie die Durchführung von Direct-Mail-Aktionen mit externen Adressen als datenschutzrechtlich bedenklich kritisiert worden. Die Ausführungen des Rundfunkdatenschutzbeauftragten zu diesen Punkten können wie folgt zusammengefaßt werden:

Kreditinstitute teilen auf Anfrage der GEZ die ihnen bekanntgewordenen Anschriftenänderungen solcher Rundfunkteilnehmer mit, die ihre Gebühren vom Konto abbuchen lassen. Der Datenschutzbeauftragte stellt klar, daß es sich hierbei nicht um „Bankauskünfte" im Sinne der AGB der Banken und Sparkassen handele; solche „Bankauskünfte" beträfen die wirtschaftlichen Verhältnisse, die Kreditwürdigkeit und die Zahlungsfähigkeit des Kunden. Die Mitteilung bloßer Anschriftenänderungen sei vielmehr nach § 24 Abs. 1 BDSG unter den dort genannten Voraussetzungen zulässig. Die GEZ habe die notwendigen Vorkehrungen getroffen, um Problemfälle auszuschließen. In anderen Fällen, in denen Briefe mit dem Vermerk „unbekannt verzogen" zurückkommen, holt die GEZ Auskünfte aus dem Melderegister ein. Die in diesem Zusammenhang in der Medienberichterstattung aufgestellte Behauptung, die GEZ arbeite mit einer „unzulässigen Rasterfahndung" durch elektronischen Datenabgleich mit den kompletten Einwohnermelderegistern der Städte, weist der Datenschutzbeauftragte als unzutreffend zurück. Ein derartiger Datenabgleich finde nicht statt. Die GEZ hole nur Einzelauskünfte ein, die zu beantworten zu den gesetzlichen Aufgaben der Melderegister gehöre. Die monatlich ca. 1.200 Einzelauskünfte der Landeshauptstadt München werden künftig anstelle des bisherigen schriftlichen Verfahrens im Wege des Austauschs von Datenträgern erteilt; dies bedeute sowohl für die GEZ als auch für die Stadt eine wesentlich rationellere Bearbeitung.

Über Direct-Mail-Aktionen der GEZ war bereits im letzten Tätigkeitsbericht berichtet worden. Im Berichtszeitraum fanden zwei Tests mit Verfahren der Direktwerbung statt. In einem Fall wurden mit Hilfe eines externen, angemieteten Adressenmaterials Personen, deren Adressen im Teilnehmerbestand der GEZ nicht geführt waren, angeschrieben und um freiwillige Meldung einer etwa geänderten Adresse oder etwaiger nicht gemeldeter Rundfunkgeräte gebeten. Bei dem anderen Test wurden abgemeldete Teilnehmer ca. 1 Jahr nach ihrer Abmeldung – unmittelbar vor Löschung der Teilnehmerdaten – angeschrieben und um Anmeldung etwa wieder aufgestellter Rundfunkgeräte gebeten. Der Datenschutzbeauftragte hebt hervor, daß es sich in beiden Fällen um datenschutzrechtlich zulässige reine Werbemaßnahmen gehandelt habe. Weder für den Fall, daß der Angeschriebene auf ein Anschreiben nicht reagiert, noch für den Fall, daß er sich daraufhin freiwillig anmeldet, dürften irgendwelche hoheitliche Maßnahmen gegen ihn ergriffen werden. Die Tests hätten im übrigen gute Erfolge gezeigt und würden voraussichtlich von der GEZ als Normalverfahren weitergeführt.

Der Datenschutzbeauftragte geht in seinem Tätigkeitsbericht ferner auf den beabsichtigten Einsatz des neuen Dienstes Bildschirmtext (Btx) für den Runkfunkgebühreneinzug ein. Als äußerst problematisch für die GEZ und die Runkfunkanstalten erscheint dem Datenschutzbeauftragten insoweit die Regelung der Datenschutzaufsicht über Btx-Anbieter, da die einzelnen landesrechtlichen Regelungen teilweise unterschiedliche Aufsichtsinstanzen für die Datenschutzkontrolle vorsehen. Schließlich berichtet der Datenschutzbeauftragte über technische und organisatorische Maßnahmen zur Verbesserung des Datenschutzes bei der GEZ sowie über die Erarbeitung eines Konzeptes für eine zeitgemäße Datenkommunikation zwischen der GEZ und den Rundfunkanstalten. Der Datenschutzbeauftragte des Bayerischen Rundfunks weist abschließend darauf hin, daß es auch im Jahr 1984 keinen Anlaß für eine förmliche Beanstandung gegeben habe.

22. Weiterentwicklung des Datenschutzrechts

22.1. Umsetzung des informationellen Selbstbestimmungsrechts

Im Bereich der Gesetzgebung

Auf Antrag des Abgeordneten Regensburger hat der **Bayer. Landtag** folgenden Beschluß gefaßt:

„Die Staatsregierung wird ersucht,

1. zu prüfen und umgehend zu berichten, welche Konsequenzen sich aus dem Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 über die Verfassungsbeschwerde gegen das Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung vom 25. März 1983 für die bayerische Gesetzgebung und Verwaltungspraxis ergeben,
2. notwendige Vorschläge zu Gesetzesänderungen alsbald dem Landtag vorzulegen und

3. zu berichten, wie sie die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 1984 zu den Auswirkungen des Volkszählungsurteils beurteilt."

Der **Bayerische Senat** hat auf Antrag der Senatoren Dr. Schumann, Deffner, Gebhard, Dr. Hermann und Paulus am 21.2.1985 folgenden Beschluß gefaßt (Sen-Drs. Nr. 26/85):

„Die Bayerische Staatsregierung wird ersucht, in Zukunft bei Gesetzentwürfen nicht nur die Frage nach Kosten und Alternativen der vorgesehenen Regelungen anzusprechen, sondern kurz auf die Auswirkungen des Gesetzvorhabens auf Erhebung und Nutzung personenbezogener Daten einzugehen.

Begründung:
Zahlreiche Gesetzentwürfe wirken sich auf personenbezogene Daten aus. Für die Beurteilung des Gesetzentwurfes ist es deshalb wichtig, ob und in welchem Ausmaß solche Auswirkungen bestehen. Der Bayerische Landesbeauftragte für den Datenschutz hat sowohl in seinem 5. Tätigkeitsbericht (Drs. 10/1664, Ziff. 1.3, Seite 6, am Ende) als auch in seinem 6. Tätigkeitsbericht (Drs. 10/4383, Ziff. 1. Vormemerkung, am Ende, Seite 6) angeregt, im Vorblatt von Gesetzentwürfen entsprechende Angaben vorzusehen."

Um das im ersten Satz der Begründung angesprochene Ziel des Beschlusses zu erreichen, müßten in Gesetzentwürfen in aller Kürze dem Parlament die Informationen gegeben werden, die erkennen lassen,

- ob der Entwurf Auswirkungen auf personenbezogen Daten hat und gegebenenfalls
- welches diese Auswirkungen sein könnten.

Hier ist insbesondere daran zu denken, ob als Folge des Gesetz entwurfes personenbezogene Daten erhoben und gespeichert werden sollten, wie sie genutzt werden sollen, ob Übermittlungen oder sonstige Verbindungen zu anderen Stellen vorgesehen sind. Auch über die Sensibilität der Daten d.h. den Grad eines evtl. mit der Datenverarbeitung verbundenen Risikos wären hier Aussagen geboten.

22.2. Fortentwicklung von BDSG und BayDSG

Der Bundestagsinnenausschuß hielt am 24. Juni 1985 eine öffentliche Anhörung zum Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes ab. Auch der Bayerische Landesbeauftragte für den Datenschutz war um eine schriftliche Stellungnahme zu einem umfangreichen Fragenkatalog gebeten worden. Die von mir bei dieser Gelegenheit schriftlich und mündlich gemachten Ausführungen beruhen auf den bei meiner bisherigen Tätigkeit gemachten Erfahrungen. Aus ihnen sei an dieser Stelle angeführt:

22.2.1. Notwendigkeit ergänzender Regelungen

Eingangs meiner Stellungnahme wies ich auf die meines Erachtens bestehende Notwendigkeit hin, wegen der inzwischen eingetretenen technischen Fortentwicklung das Datenschutzrecht grundlegend zu revidieren (siehe 6. Tätigkeitsbericht Nr. 3 Seite 15 bis 17). Zu der Frage, in welcher Art eine Anpassung des Datenschutzrechts an die eingetretenen Fortentwicklung erfolgen sollte, habe ich ausgeführt:

Ergänzende Verfahrensregelungen:

Bevor umfangreiche EDV-Verfahren entwickelt werden oder bei deren wesentlicher Änderung sollte ein Prüfverfahren durchlaufen werden, in dem die Notwendigkeit der Automatisierung und die zu erwartenden Risiken für das informationelle Selbstbestimmungsrecht der Betroffenen gegeneinander abgewogen werden. Ein solches Prüfverfahren müßte im BDSG institutionalisiert werden.

Es ist bekannt, daß von umfangreicheren neuen DV-Verfahren Wirkungen ausgehen können, die das informationelle Selbstbestimmungsrecht vieler Betroffener berühren können. So wäre z.B die Einrichtung von Registern über Personen, die an einer bestimmten Krankheit leiden, oder auch von allgemeinen Krankheitsregistern für alle Erkrankten eine Maßnahme, die bereits wegen der Sensibilität der Daten erhebliche Risiken erzeugen könnte – beispielsweise im Zusammenhang mit Kreditwürdigkeit oder mit den Chancen bei der Suche nach einem Arbeitsplatz. Die Berührung des informationellen Selbstbestimmungsrechts könnte auch darin liegen, daß solche umfassende Datensammlungen zu extensiv genutzt werden. Dabei gilt es nicht nur die Gefahr einer mißbräuchlich zu weit gehenden Nutzung zu bannen, sondern auch den Trend zur „legalen" Ausweitung von Nutzungsmöglichkeiten in die Überlegungen mit einzubeziehen. Erfahrungsgemäß entsteht nach der Errichtung jeder größeren Datensammlung ein Druck, weitere zunächst nicht vorgesehene Nutzungen zuzulassen.

Im Interesse der Betroffenen müßte nun möglichst schon bei der Planung solcher Datensammlungen Vorsorge getroffen werden, daß sie sich nicht zum Nachteil der Betroffenen extensiv nutzen lassen.

Die problematischen Wirkungen insbesondere von größeren Datenverarbeitungsverfahren könnten wohl bei intensiver Vorprüfung solcher Vorhaben weitgehend aufgedeckt werden. Voraussetzung wäre eine fachübergreifende Erhebung der Risiken (ähnlich dem Planfeststellungsverfahren z.B. bei größeren Straßenbauten). Eine solche fachübergreifende systematische Erörterung der Risiken größerer DV-Systeme wird jedoch meines Wissens gegenwärtig vor deren Entwicklung und Einführung nicht durchgeführt. Einen bemerkenswerten Ansatz in dieser Richtung enthält allerdings Art. 26 Abs. 2 und 4 des Bayerischen Datenschutzgesetzes. Danach ist eine besondere datenschutzrechtliche Freigabe der Datensätze für die Speicherung und die regelmäßige Datenübermittlung durch die oberste Dienstbehörde erforderlich und deren Mitteilung an den Landesbeauftragten für den Datenschutz. Allerdings ist dieses Verfahren meines Erachtens noch kein hinreichender Ersatz für ein umfassende fachübergreifende Abklärung möglicher Risiken von größeren DV-Verfahren im Sinne einer Erörterung von Technologiefolgen.

Das Bundesdatenschutzgesetz sollte daher eine solche fachübergreifende Risikoprüfung für größere DV-Verfahren vorsehen.

Ergänzende materielle Regelungen:

Ergänzend zu verfahrensmäßigen Vorschriften, die eine hinreichende, evtl. auch öffentliche Auseinandersetzung mit möglichen Folgen der Datenverarbeitung und eine Festlegung ihrer Grenzen zum Gegenstand haben könnten, wäre aber auch an materielle Anforderungen zu denken, die im Bundesdatenschutzgesetz festgelegt werden könnten. Das Volkszählungsurteil des Bundesverfassungsgerichts gibt hierzu, wie ich meine, einen wesentlichen Anstoß: Es wendet sich gegen eine „unbegrenzte" Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten (Leitsatz 1 des Urteils).

Hieraus könnte die folgende materielle Anforderung für eine Begrenzung von Datenverarbeitung gewonnen werden: Datenverarbeitung sollte nicht zulässig sein, wenn sie in verfassungsrechtlich problematischer Weise zur Erstellung von Persönlichkeitsprofilen führen könnte, bzw., wie das Gericht ausführt, zur Herstellung von solchen „Teilabbildern" der Person, die mit der Würde des Menschen nicht vereinbar wären. Zu denken wäre zum Beispiel an eine Zusammenführung von Informationen aus verschiedenen Sparten einer Großstadtverwaltung über ein und denselben Bürger in einem einzigen Informationszusammenhang (Pläne hierzu sind noch nicht bekannt geworden, die gemeinsame Datenverarbeitung in einem Rechenzentrum könnte hierzu jedoch Anstöße geben).

Aus dem Begrenzungsgebot würden sich wohl auch Anforderungen auf DV-organisatorische und DV-technische Trennung von Informationsbereichen ergeben, deren ungetrennte Verarbeitung unzulässige Persönlichkeitsprofile entstehen lassen könnte. Ich hielte es für einen voreiligen Schluß anzunehmen, daß im technisch-organisatorischen Bereich hier alle Fragen mit der Vergabe entsprechender Zugriffsberechtigungen gelöst werden könnten. Allein die Speicherung umfassender Informationen über eine Person auf einem DV-System wäre unter Umständen bereits als Schaffung eines solchen problematischen Profils zu betrachten, auch wenn die Vergabe unterschiedlicher Zugriffsberechtigungen vorgesehen ist.

Zu untersuchen wäre auch, ob durch eine materielle Regelung im BDSG die Entstehung solcher Datensammlungen verhindert oder begrenzt werden könnte, deren Nutzung dazu führen könnte, daß Betroffene von der Ausnützung von Grundrechten Abstand nehmen. Die Begründung des Volkszählungsgesetzes gibt ja einen deutlichen Hinweis in diese Richtung. Zur Klärung dieser Frage wären allerdings noch gründliche Erhebungen und Erörterungen notwendig. Möglicherweise könnte aber ein evtl. Gefahrenpotential zunächst durch gründliche Untersuchungen von geplanten DV-Verfahren – wie oben vorgeschlagen – aufgedeckt und durch konkrete Auflagen und Bedingungen von vorneherein gebannt werden.

Ich hielte es aus grundsätzlichen Erwägungen für sinnvoll, entsprechende Anforderungen im Bundesdatenschutzgesetz (und in den Landesdatenschutzgesetzen) vorzusehen, um zu vermeiden, daß verwaltungsorganisatorische Ausgestaltungsüberlegungen jeweils nur an Art. 1 und 2 Grundgesetz und der hierzu ergangenen Rechtsprechung zu messen wären.

Drei wichtige Punkte:

Aus der Vielzahl der Punkte, zu denen gegenüber dem Bundestags-Innenausschuß Stellung zu nehmen war, seien im folgenden drei besonders wichtig erscheinende wiedergegeben:

- Die Erstreckung des Anwendungsbereichs des Gesetzes auf Da tenverarbeitung außerhalb von Dateien,
- die Einführung von Zweckbindungsregelungen und
- die Kontrollzuständigkeit der Datenschutzbeauftragten

22.2.2. Anwendungsbereich des BDSG:

Zur Frage der Erstreckung des Anwendungsbereiches des Bundesdatenschutzgesetzes auf Datenverarbeitung außerhalb von Dateien, namentlich in Akten und anderen Darstellungsformen, z.B. Videoaufzeichnungen:

a) **Für automatisierte Verfahren,** auf die der bisherige „Datei"-Begriff nicht mehr paßt:

Der Anwendungsbereich der Datenschutzgesetze stellt heute in erster Linie auf den Dateibegriff und damit auf die Voraussetzungen des „gleichartigen Aufbaus" und der „Sortierbarkeit" von Daten ab. Dagegen setzen moderne DV-Techniken bei Datenverwaltungssystemen zunehmend den gleichartigen Aufbau der gespeicherten Informationen nicht mehr voraus. Die Informationswiedergewinnung kann dabei auch durch ein Durchsuchen des Bestandes nach bestimmten Kriterien ohne Sortieren oder Umsortieren erfolgen.

Durch die rasche Entwicklung der Datenverarbeitung hin zur Kommunikationstechnik werden außerdem zunehmend maschinell gespeicherte personenbezogene Informationen, die durchaus sensible und schutzbedürftige Daten enthalten können, nicht mehr von den Datenschutzgesetzen erfaßt. In erster Linie sind hier digitalisierte Kommunikation zu nennen, in der Texte, Sprache und Bilder gespeichert, verarbeitet und übertragen werden können und verschiedene Formen der Volltextverarbeitung.

Deshalb muß jedenfalls bei automatisierter Datenverarbeitung der Dateibegriff als Anwendungsvoraussetzung des Gesetzes entfallen. Sollte sich der Gesetzgeber hierzu nicht durchringen können, müßte bei der Definition des Dateibegriffes für automatische Verfahren auf die Eigenschaften des gleichartigen Aufbaus (Formatierung) und der Sortierbarkeit verzichtet werden.

Daß gerade bei den „Neuen Medien" der Dateibegriff herkömmlicher Art auf Schwierigkeiten bei einer sinnvollen Anwendung des Datenschutzrechts führen kann, zeigt die Regelung in Art. 9 Abs. 5 Btx-StV, in der durch eine Fiktion eine Datensammlung zur Datei gemacht wird.

b) Für **indirekt automatisierte** Verfahren:

Für die durch Datenverarbeitung erschließbaren Aktenbestände sollte eine Klarstellung erfolgen; eine Beschränkung der Anwendung des BDSG auf den Inhalt einer eventuellen Suchdatei, die aus den Akten herausgezogene Suchkriterien für das Auffinden der

Akten enthält, wäre eine unnötige Regelung, da die automatisiert geführten Suchkriterien ohnehin unter den Dateibegriff fallen. Erforderlich wäre aber klarzustellen, inwieweit das BDSG auch auf nicht maschinenlesbar gespeicherte Daten, die über maschinenlesbar gespeicherte Daten auffindbar gemacht wurden, anzuwenden sein soll. Soweit durch automatisierte Datenverarbeitung die Verfügbarkeit solcher nicht maschinenlesbaren Informationen erheblich erhöht wird, wäre meines Erachtens die Anwendung des Gesetzes vorzusehen. Im übrigen müßte die Anwendung von Regelungen des Allgemeinen

Verwaltungsverfahrensrechts genügen.

c) **Für Akten:**

Da das Bundesverfassungsgericht hinsichtlich der informationellen Selbstbestimmung nicht nach der Speicherungsart unterscheidet, müßten Regelungen zum Schutz des informationellen Selbstbestimmungsrechts beim Umgang mit personenbezogenen Daten in Akten grundsätzlich die gleichen Schutzwirkungen für den Betroffenen enthalten, wie die Regelungen des Datenschutzgesetzes für Dateien. Unterschiedlichen Gefährdungslagen bei Akten und Dateien (bzw. automatisierten Verfah rens) kann dabei mit unterschiedlichen Maßnahmen zur Erreichung der gebotenen Schutzwirkung Rechnung getragen werden.

d) **Für andere Darstellungsformen:**

Foto- und Video-Aufnahmen von Personen können grundrechtseinschränkend wirken, wie das Beispiel der Demonstrationsteilnahme im Volkszählungsurteil zeigt. Da es sich im dort zitierten Fall primär um eine sehr schwierige und exakt zu treffende Güterabwägung zwischen Sicherheits- und Persönlichkeitsinteressen handelt, sollte vor allem eine bereichsspezifische Regelung für die Sicherheitsbehörden vorgesehen werden.

Die Frage ist, ob entsprechende Aufzeichnungen durch andere Behörden im allgemeinen Datenschutzgesetz zu regeln wären. Aus meiner Prüftätigkeit ist mir hierzu ein Beschwerdebeispiel bekannt, in dem sich der Petent dadurch in seinen Rechten beeinträchtigt fühlte, daß eine Gemeinde in einer Bürgerversammlung einzelne Debattenredner fotografieren ließ, was den Entschluß, sich in der Debatte zu Wort zu melden, möglicherweise erschwerte. Die Regelungen des Kunsturhebergesetzes über das Recht am eigenen Bild betreffen primär die Veröffentlichung und Zurschaustellung von Aufnahmen und sehen hierfür eine Einwilligungslösung vor. Sie erweisen sich damit kaum als wirksames Mittel gegen das Fotografieren – soweit dieses auf die Rechtsausübung hemmend wirken kann.

Im Zusammenhang mit Fotoaufnahmen wäre im übrigen zu berücksichtigen, ob sie im einzelnen Fall personenbezogen, zum Beispiel namentlich (evtl. auch dateimäßig) erschlossen sind. Im übrigen sollten sie als „Angaben zur Person" ohnehin unter den Anwendungsbereich des Bundesdatenschutzgesetzes fallen.

22.2.3. Zur Einführung von Zweckbindungsregelungen:

a) **Allgemeines:**

Das Bundesdatenschutzgesetz sollte eine generelle Regelung zur Zweckbindung enthalten. Daneben sollten dort bereichsspezifische Regelungen für die Bereiche erlassen werden, in denen die Verarbeitung personenbezogener Daten das informationelle Selbstbestimmungsrecht des Betroffenen stärker berührt. Hierzu zählt m. E. die Datenverarbeitung im Rahmen der Sicherheitsbehörden, der Neuen Medien, des Gesundheitswesens (außerhalb des Bereiches des behandelnden Arztes) sowie der Sozialbehörden.

Die oben genannte generelle Regelung für die Zweckbindung im Bundesdatenschutzgesetz müßte so gestaltet sein, daß sie Raum für sinnvolle und sachlich gebotene entsprechende bereichsspezifische Regelungen läßt.

b) **Materielle Anforderungen an die Zweckbindungsregelung:**

Wie bisher müßte die Zweckbindung bewirken, daß besondere Berufs- oder Amtsgeheimnisse verlängert und dürfte nicht durch eine allgemeine Zulässigkeitsregelung ersetzt werden, die lediglich die Erforderlichkeit der Daten für den Empfänger prüft.

Unerhebliche Zweckänderungen, die keine belastenden Wirkungen für den Betroffenen erzeugen, dürften nicht behindert werden. Erst recht gilt dies bei den Betroffenen entlastenden Wirkungen von Zweckänderungen, da sich sonst der Nutzen der Zweckbindung in einen Nachteil verkehren würde. Allerdings darf ein möglicher Nutzen der im Weiterleiten der Daten für andere Zwecke gesehen werden kann, nicht von vorneherein dem Interesse des Betroffenen an der Zweckbindung übergeordnet werden.

Dagegen wäre bei erheblichen Belastungen des Betroffenen durch eine Zweckänderung eine absolute Zweckbindung vorzusehen, die die schon bestehenden besonderen Amtsgeheimnisse und deren „Verlängerung" ergänzen würde.

Soweit der Bürger Daten freiwillig für einen bestimmten Zweck angegeben hat, muß eine Zweckänderung grundsätzlich ausscheiden.

Meines Erachtens sollte eine Regelung nach den vorgenannten Grundsätzen auf die Interessenssphäre des Betroffenen abstellen. Aus der Sicht der Verwaltung wäre es gleichwohl wünschenswert, Ausnahmen für Fälle vorzusehen, in denen ein und dieselbe Dienststelle Angaben über den Betroffenen auch für einen anderen Zweck braucht. Würde dabei der Begriff der Dienststelle nicht zu weit gezogen und wären die Nutzungszwecke nicht zu heterogen, wäre aus der Sicht des Betroffenen dagegen wohl kaum etwas einzuwenden. Für problematisch hielte ich es jedoch grundsätzlich, eine allgemeine Ausnahme für Datennutzung für andere Zwecke bei anderen Dienststellen vorzusehen.

Die Regelung im BDSG müßte also Zweckänderungen ausschließen, wenn durch sie der Betroffene erheblich belastet würde. Sie könnte dagegen ggf. bereichsspezi-

fisch – unter Beachtung des Verhältnismäßigkeitsgrundsatzes – zugelassen sein, oder die erforderlichen Daten müßten durch Erhebung beim Betroffenen für den neuen Zweck oder durch Datenübermittlung von einer Behörde oder Stelle, für die diese Datenübermittlung keine erhebliche Zweckänderung wäre, beschafft werden.

Ganz allgemein gilt, daß Zweckänderungen weder zu Persönlichkeitsprofilen führen, noch die vom Bundesverfassungsgericht in mehreren Entscheidungen aus der Verfassung abgeleiteten Grenzen der Datenverarbeitung durchbrechen dürfen.

c) **Kontrollierbarkeit der Zweckbindung:**

Die Kontrollierbarkeit der Zweckbindung setzt jeweils Klarheit über den Zweck voraus, auf den sich die Bindung bezieht. Ich gehe davon aus, daß eine automatisierte Überwachung des Zweck bindungsgebots zunächst nicht möglich, aber auch nicht erforderlich wäre. Die Kontrollierbarkeit setzt eine automatisierte Speicherung des Zwecks nicht voraus. Die Kontrolle müßte also keinen übertriebenen Aufwand erzeugen.

Die Prüfung der Zweckbindung muß immer am Anfang der Datenverarbeitung stehen. Eine nur schematische, quasi automatisierte Prüfung der Zweckbindung würde wohl nicht genügen.

d) **Unterschiedliche Regelung der Zweckbindung für Nutzung und Übermittlung von Daten?**

Ich halte die Unterscheidung in der Fragestellung zwischen Nutzung und Übermittlung nicht für geboten. Würde nämlich in die ser Art in einer gesetzlichen Regelung differenziert, so würde der umstrittene Begriff der speichernden Stelle und der Datenübermittlung, der durch die Novelle möglicherweise nicht geklärt wird (siehe oben, Beispiel der speichernden Stelle und Datenübermittlung innerhalb einer Behörde mit großem Aufgabenspektrum), eine nicht überschaubare Wirkung auf die Regelung der Zweckbindung erlangen. So würden etwa in einer Großstadt, je nachdem, ob sie insgesamt als eine speichernde Stelle betrachtet würde, oder als Bündelung einer Vielzahl solcher Stellen, unterschiedliche Regeln zur Zweckbindung gelten. Tatsächlich kann materiell jedoch nur ausschlaggebend sein, inwieweit eine Zweckänderung das informationelle Selbstbestimmungsrecht berührt, nicht aber, ob sie innerhalb einer speichernden Stelle oder außerhalb derselben vor sich geht.

22.2.4. Zur Frage der Kontrollzuständigkeit des Bundes- bzw. Landesbeauftragten für den Datenschutz:

a) **Zur derzeitigen Rechtslage:**

Anlaß für die Schaffung des BDSG und damit auch der Institution eines Bundesbeauftragten für den Datenschutz (und entsprechend der Institutionen der Landesbeauftragten für den Datenschutz) war der immer stärker zunehmende Einsatz automatisierter Datenverarbeitung in der öffentlichen Verwaltung. Das Bundesverfassungsgericht hat im Volkszählungsgesetz darüber hinaus der Tätigkeit unabhängiger Datenschutzbeauftragter „auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen" erhebliche Bedeutung für einen effektiven Schutz des „Rechts auf informationelle Selbstbestimmung" beigemessen.

Die danach zur Wahrung der Rechte aus Art. 1 und 2 GG gebotene „Gewährleistung eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen" setzt eine umfassende Kontrollkompetenz des Bundesbeauftragten für den Datenschutz – wie auch der Landesbeauftragten – voraus. Sie bezieht im BDSG (und auch im BayDSG) schon jetzt zu Recht auch nichtautomatisierte Dateien in die Kontrolle des Datenschutzbeauftragten ein, weil das Argument der im Verhältnis zu Akten erhöhten Verfügbarkeit dieser Daten (z. B. in Karteien) auch auf diese zutrifft, und weil sich in vielen Fällen automatisierte und nichtautomatisierte Datenhaltung in einer Weise ergänzen, die es unverständlich erscheinen ließe, wenn die Kontrolle eines die Betroffenen insgesamt berührenden Datenverarbeitungsvorgangs vor dem nichtautomatisierten Teil dieses Vorgangs haltmachen würde.

Nicht zuletzt aus diesem Grund wird den Vorschriften des Bayerischen Datenschutzgesetzes entnommen, daß die Aufgabe des Datenschutzbeauftragten: „..überwacht die Einhaltung des Datenschutzes bei allen öffentlichen Stellen" (Art. 28 Abs. 1 BayDSG) die Kontrolle der Einhaltung von Datenschutzvorschriften in anderen Gesetzen als dem BayDSG (z. B. ärztliche Schweige pflicht, SGB) auch dann umfaßt, wenn entsprechende personenbezogene Daten nicht in Dateiform vorgehalten werden. Das Bundesverfassungsgericht hat im Hinblick auf Art. 2 Abs. 1 und 1 Abs. 2 GG im übrigen das informationelle Selbstbestimmungsrecht nicht auf ein bestimmtes Speichermedium beschränkt. Für die umfassende Erstreckung der Kontrollzuständigkeit spricht außer dem,

- daß der Übergang von Dateiform zur Nichtdateiform oft fließend ist (z. B. „Fieberkurve"),
- daß eine Vielzahl besonders sensibler personenbezogener Daten in nichtformatierter Form in Akten oder in Zwischenformen zwischen Akten und Dateien vorgehalten werden, deren Schutzbedürftigkeit dem Inhalt von Dateien nicht nur nicht nachsteht, sondern sie oft wesentlich überschreitet, und
- daß die Bevölkerung, insbesondere der einzelne Betroffene, keinerlei Verständnis dafür aufbringt, daß die Kontrolle durch den unabhängigen Datenschutzbeauftragten, also durch eine keinen Interessenkollisionen ausgesetzte Instanz, davon abhängig sein soll, daß die zu schützenden Daten in einer bestimmten Form auf einem Datenträger vorgehalten werden.

In meiner Kontrollpraxis ließ ich mich bei der Prüfung von Akten ohne unmittelbaren Dateibezug von folgenden Grundsätzen leiten:

Aus der Sicht des Datenschutzes galt es festzustellen,

- welche Informationsströme innerhalb und außerhalb von Behörden bestehen,
- inwieweit generell Speicherung oder Übermittlung bei einer bestimmten Behörde zulässig sind oder Löschungen rechtzeitig vorgenommen werden,

– inwieweit die Weitergabe vollständiger Akten an andere Behörden regelmäßig zu Problemen führt, weil die Akten Informationen enthalten, die ihrer Natur nach von einer Übermittlung ausgeschlossen sein müßten (z. B. ärztliche Gutachten).

Bestimmte einzelne Datenverarbeitungsvorgänge in Akten prüfe ich jeweils dann, wenn entweder ein Bürger sich unmittelbar im Rahmen seines Anrufungsrechts an mich wendet, oder wenn ich auf andere Weise Anhaltspunkte zu Zweifeln an einer rechtmäßigen Datenverarbeitung im Einzelfall habe. Die Überwachung der Einhaltung des informationellen Selbstbestimmungsrechts kann meines Erachtens nicht an der Datenverarbeitung in Akten enden.

Ich bin der Überzeugung, daß meine derzeitige Praxis der Prüfung auch von Akten dem vom Gesetzgeber ursprünglich gewollten Anliegen und der im Volkszählungsurteil des Bundesverfassungsgerichts geäußerten Ansicht entspricht. Da überdies für Betroffene in besonders sensiblen Bereichen (wie gegenüber Polizei und Verfassungsschutzbehörden) kein Auskunftsanspruch besteht, ist die Anrufung des unabhängigen Datenschutzbeauftragten für sie hier eine sehr wichtige Möglichkeit, eine rasche und kostenfreie Überprüfung herbeizuführen.

b) **Ergänzung des BDSG:**

Um Zweifel über das Tätigkeitsfeld des Datenschutzbeauftragten auszuräumen, bin ich daher der Auffassung, daß die von mir oben beschriebene Kontrolltätigkeit – auch außerhalb von Dateien – im Gesetz ausdrücklich Niederschlag finden sollte. Die Kontrollmöglichkeiten des Bundesbeauftragten sollten auch Bereiche, die durch bestimmte Geheimhaltungsvorschriften geschützt sind, nicht ausschließen. Die auch im BDSG enthaltene Staatsschutzklausel (§ 19 Abs. 3 letzter Satz) gewährleistet, daß die Einsicht in Unterlagen und Akten nicht die Sicherheit des Bundes oder eines Landes gefährdet.

Gegen die vorstehend geschilderte Konzeption wird von manchen Stellen eingewandt, es handle sich um eine nicht effektive Doppelkontrolle, da die kontrollierten Stellen jeweils auch der Rechtsaufsicht von Behörden unterstehen. Diese Argumentation übersieht einen wesentlichen Punkt, der daher nochmals verdeutlicht sei: Die Einrichtung der Datenschutzbeauftragten durch die Datenschutzgesetze hatte zu einem wesentlichen Teil auch den Sinn deutlich zu machen, daß zwar die Möglichkeiten automatisierter und herkömmlicher Datenverarbeitung immer umfassender genutzt werden sollen, gleichzeitig aber eventuell daraus entstehende Nachteile durch ein besonderes, dafür neugeschaffenes Instrument ausgeglichen werden sollen. Dieses Instrument ist der Datenschutzbeauftragte. Er wurde speziell hierfür mit einer unabhängigen Stellung ausgestattet, die die jeweilige Rechtsaufsichtsbehörde, die sich mit der Frage der Zulässigkeit der Datenverarbeitung selbstverständlich ebenfalls befassen kann, nicht besitzt. Zwar ist deren Handeln durch die Tätigkeit unabhängiger Gerichte überprüfbar, doch sollte durch die Datenschutzgesetze erkennbar dem Betroffenen eine schnelle („möglichst unbürokratische") Hilfe ohne den Zeit- und u. U. Kostenaufwand des Klageweges an die Hand gegeben werden. Es darf daher nicht in Vergessenheit geraten, daß sich die Einrichtung der Datenschutzbeauftragten gerade wegen ihrer Unabhängigkeit auf Dauer besser dazu eignet, Sorgen und Befürchtungen im Zusammenhang mit Datenverarbeitung in Grenzen zu halten, als dies durch Widerspruchsbehörden oder den Rechtsweg vor den Gerichten möglich ist.

23. Der Beirat

Über die Einrichtung und die Aufgaben des gemäß Art. 29 BayDSG beim Landesbeauftragten für den Datenschutz gebildeten Beirats finden sich ausführliche Darstellungen in früheren Tätigkeitsberichten (siehe insbesondere 5. TB Textziffer 2.1, S. 7). Im Rahmen der Anhörung des Bundestagsinnenausschusses zu Fragen der Novellierung des Bundesdatenschutzgesetzes war vom Ausschuß auch die Frage nach der Zweckmäßigkeit eines solchen Beirats gestellt worden. Bayern ist das einzige Bundesland, in dem ein Beirat besteht. Aufgrund meiner Erfahrungen habe ich in meiner Stellungnahme nachdrücklich auf die wertvolle, tatkräftige Unterstützung meiner Tätigkeit durch den Beirat hingewiesen.

Die dem Landtag angehörenden Mitglieder des Beirats werden jeweils für die Wahldauer des Landtags bestellt, die übrigen Mitglieder jeweils für 4 Jahre. Nach der Landtagswahl im Herbst 1982 sind die Mitglieder des Beirats neu bestellt worden.

Vorsitzender ist der Abgeordnete Hermann Regensburger, stellvertretender Vorsitzender der Abgeordnete Klaus Warnecke. Mitglieder des Beirats und ihre Stellvertreter sind gegenwärtig:

Die Landtagsabgeordneten:

Hermann Regensburger	Dr. Paul Wilhelm
Franz Josef Brosch	Manfred Humbs
Wolfgang Dandorfer	Johann Böhm
Franz Gruber	Konrad Kobler
Klaus Warnecke	Rolf Langenberger
Alfred Münch	Heinz Mehrlich

Die Senatoren:

Wolfgang Burnhauser	Otto Neukum

Für die Staatsregierung:

Dr. Friedrich Giehl Ministerialdirigent im Bayer. Staatsministerium des Innern	Dr. Werner Böhme Ministerialrat im Bayer. Staatsministerium der Finanzen

Für die Kommunalen Spitzenverbände:

Dr. Georg Wilhelm Geschäftsleitender Direktor der Anstalt für Kommunale Datenverarbeitung in Bayern	Klaus Eichhorn Ltd. Verwaltungsdirektor der Anstalt für Kommunale Datenverarbeitung in Bayern

Für die Sozialversicherungsträger:

Franz-Martin Fehn Erster Direktor der Landesversicherungs- anstalt Oberfranken und Mittelfranken	Herbert Schmaus Verwaltungsdirektor beim Landesverband der Orts krankenkassen in Bayern

Für den Verband der Freien Berufe in Bayern e.V.:

Dr. med. H. Braun Präsident des Verbandes Freier Berufe in Bayern e.V.	Winfried Wachter Präsidiumsmitglied des Verbandes Freier Berufe in Bayern e.V.

Im Berichtsjahr tagte der Beirat viermal, nämlich am 24. Januar, 21. Februar, 17. Juli und 13. November 1984. Er befaßte sich in seinen Sitzungen mit folgenden Punkten:

- Datenschutzrechtliche Beanstandungen bei Bayer. Behörden,
- Urteil des Bundesverfassungsgerichts zum Volkszählungs gesetz 1983,
- Datenschutzforderungen für ein Bayer. Personalausweisgesetz,
- Anordnung über Mitteilungen in Strafsachen (MiStra) – siehe unten,
- Bericht über ein Modellversuch zur computergesteuerten Wirtschaftlichkeitsprüfung bei gesetzlichen Krankenkassen,
- Bayer. Medienerprobungs- und -entwicklungsgesetz,
- Veröffentlichung eines Nachtrags zur Übersicht über das Datenschutzregister,
- Datenschutzkontrollen im technisch-organisatorischen Bereich,
- Weitergabe des Anschriftenverzeichnisses der Kreisräte an Dritte,
- Sonderaktion „Aktenbereinigung" beim Bayer. Landeskriminalamt
- Vorberatung des Tätigkeitsberichts 1983 des Landesbeauftragten für den Datenschutz gem. Art. 28 Abs. 6 BayDSG,
- Auskunft aus dem Melderegister über Wahlberechtigte an Parteien und Wählergruppen gem. Art. 35 Abs. 1 MeldeG,
- Wegen der stark gewachsenen Arbeitsbelastung des Datenschutzbeauftragten und der zu erwartenden zusätzlichen Arbeit im Zusammenhang mit der Einführung neuer Medien: Unterstützung des Landesbeauftragten in seinem Bemühen drei weitere Planstellen für Mitarbeiter in seiner Geschäftsstelle im Haushalt zu erhalten,
- Entwurf der Bayer. Meldedatenübermittlungsverordnung,
- Unterrichtung über Datenschutzgesichtspunkte in der gemeinsamen Bekanntmachung der Bayer. Staatsministerien für Wirtschaft und Verkehr, des Innern und für Arbeit und Sozialordnung vom 1.8.1984 über „Bekämpfung von Schwarzarbeit",
- Problem der Übermittlung von Statistikeinzeldaten an andere Stellen im Hinblick auf die Auswirkungen des Volkszählungsurteils,
- Sachstandsbericht zur Anordnung über Mitteilungen in Zivilsachen (MiZi),
- Trennung der Bearbeitung von Beihilfeanträgen in Krankheitsfällen von der Personalsachbearbeitung, Ausnahmen vom Verbot, Beihilfedaten für andere als Beihilfezwecke zu nutzen,
- Beachtung des Datenschutzes bei Erhebungen zu der Körperschaftssteuer-Statistik,
- freiwillige gemeindliche Zusatzerhebung zur Gebäudevorerhebung,
- Erforderlichkeit von Dienstreisen sowie des Einsatzes von Dienstwagen zur unabhängigen Erfüllung von Kontrollaufgaben des Landesbeauftragten für den Datenschutz,

Über die einzelnen im Beirat erörterten Themen finden sich in diesem Bericht jeweils im entsprechenden Sachzusammenhang nähere Ausführungen. Aus den Beratungen seien jedoch zwei Besonderheiten berichtet:

- Als Ergebnis der Erörterungen zur Anordnung über die „Mitteilungen in Strafsachen (MiStra)", an denen auch Vertreter des Bayer. Staatsministerium der Justiz teilnahmen, wurde vom Beirat der folgende Beschlußvorschlag des Vorsitzenden MdL Regensburger angenommen:

  „1. Der Beirat unterstützt im Grundsatz die Stellungnahme der Datenschutzbeauftragten des Bundes und der Länder zum Entwurf der MiStra.

  2. Der Beirat hält eine Überprüfung der MiStra in der Fassung des Entwurfs der Justizverwaltungen anhand der Grundsätze des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 für notwendig.

  3. Der Beirat bittet, die Staatsregierung darauf hinzuwirken, daß

     a) eine Rechtsgrundlage für die MiStra geschaffen wird, soweit eine solche nicht schon besteht;

     b) die Beachtung der Zweckbindung in allen Mitteilungsfällen sichergestellt wird,

     c) in den Fällen, in denen ein Entscheidungsspielraum besteht, die Entscheidung durch einen Richter oder einen Staatsanwalt erfolgt;

     d) Mitteilungen grundsätzlich erst nach rechtskräftigem Abschluß des Strafverfahrens erfolgen und

     e) der Betroffene grundsätzlich von Mitteilungen benachrichtigt wird."

- Bei der Erörterung des Entwurfs einer Bayerischen Meldedatenübermittlungsverordnung ergab sich die Situation, daß in der Beiratssitzung am 13.11.1984 noch keine Entwurfsfassung für die Beratung zur Verfügung stand. Da die Verordnung zum 1. Januar 1985 in Kraft treten sollte, war gleichwohl Eile geboten. Zwischen dem Bayer. Staatsministerium des Innern und dem Landesbeauftragten für den Datenschutz bestanden aber noch Meinungsverschiedenheiten über einige Punkte des Vorentwurfs. Der Beirat hat trotz der gebotenen Eile die Beratung des Punktes vertagt und beschlossen, eine Sondersitzung dann einzuberufen, wenn zwischen dem Staatsministeriums des Innern und dem Landesbeauf-

tragten in wesentlichen Punkten keine Übereinstimmung erzielt werden könnte. Im Hinblick auf Verbesserungen aus der Sicht des Datenschutzes, die dann noch erreicht wurden, entfiel die Sondersitzung. Dem Beirat wurde abschließend in der folgenden regulären Sitzung im Jahre 1985 berichtet.

Zur Tätigkeit des Beirats siehe im übrigen in den Tätigkeitsberichten I unter 1.4, II unter 1.3, III unter 1.2.1, IV unter 1.5, V unter 2.1 sowie VI unter 1.1.

24. Behandlung des sechsten Tätigkeitsberichts im Parlament

Der Tätigkeitsbericht für 1983 wurde am 28.11.1984 im Ausschuß für Verfassungs-, Rechts- und Kommunalfragen des Landtags und am 9.1.1985 im Rechts- und Verfassungsausschuß des Bayerischen Senats beraten.

1. Im Bayerischen Landtag wies der Berichterstatter, Abgeordneter Hermann Regensburger, zunächst auf die Rolle des Beirats beim Landesbeautragten für den Datenschutz hin. Dieser habe sich in den vergangenen Jahren außerordentlich bewährt, weil durch seine Zusammensetzung gewährleistet sei, daß Datenschutzfragen sachkundig und ausgewogen diskutiert würden.

   Der Berichterstatter betonte die Bedeutung des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz. Mit dem darin anerkannten Recht auf informationelle Selbstbestimmung werde deutlich, daß sich der Datenschutz keineswegs nur auf in Dateien gespeicherte Daten beschränke. Er wies darauf hin, daß der Datenschutz in Bayern aber schon bisher keineswegs in dieser engen Betrachtungsweise verstanden worden sei.

   Er ging dann auf die Arbeiten zur Änderung der Mitteilungen in Strafsachen – MiStra – ein und teilte mit, sowohl der Bayerische Senat als auch der Rechtsausschuß habe sich mit diesem Thema intensiv befaßt; er begrüßte es, daß zahlreiche Vorstellungen des Datenschutzbeauftragten in die Beratung mit den anderen Bundesländern aufgenommen worden seien.

   Im Bereich der Neuen Medien betonte der Berichterstatter den Stellenwert des Datenschutzes und wies darauf hin, daß Versäumnisse in diesem Bereich nicht zuletzt auch zu Lasten der Akzeptanz der Bürger gingen.

   MdL Regensburger stellte fest, daß im Polizeibereich im Berichtszeitraum nur zwei Verstöße wegen unzulässigen Datenabrufs durch Polizeibeamte zu Beanstandungen geführt hätten und hob hervor, daß die Polizei in Sachen Datenschutz vorsichtig verfahre.

   Zur Schaffung eines Krebsregisters führte der Berichterstatter aus, daß sich die Datenschutzbeauftragten hinsichtlich der Notwendigkeit eines solchen Registers neutral verhielten, allerdings die Beachtung datenschutzrechtlicher Belange forderten, wenn ein solches Krebsregister geschaffen würde. Im Anschluß daran stellte er die Arbeiten an einem Archivgesetz dar und betonte, dies werde Gegenstand parlarmentarischer Beratungen sein.

   Abschließend stellte MdL Regensburger fest, daß der 6. Tätigkeitsbericht keine Hinweise auf schwerwiegende Verstöße gegen Datenschutzbestimmungen enthalte. In Bayern bestehe erfreulicherweise ein besonderes Vertrauensverhältnis zwischen dem Bayerischen Landesbeauftragten für den Datenschutz und den Verwaltungen.

   Mitberichterstatter Abgeordneter Klaus Warnecke führte aus, Datenschutz beschränke sich nicht allein darauf, die mißbräuchliche Verwendung legitimerweise angesammelter Daten zu verhindern; die Bürger müßten davor geschützt werden, daß Daten in zu großer Menge und unkontrolliert erhoben würden. Die Daten dürften nicht unkontrolliert und ungesteuert in verschiedene Kanäle fließen. Das Bundesverfassungsgericht betone im Volkszählungsurteil zu recht, daß im Zeitalter der automatischen Datenverarbeitung kein einziges Datum belanglos sei. In einem möglicherweise falschen Zusammenhang könne nämlich auch das belangloseste Datum für den Bürger verhängnisvoll werden. Den Tätigkeitsbericht bezeichnete MdL Warnecke in weiten Teilen als einen Bericht über Vollzugsdefizite im Datenschutzrecht.

   MdL Warnecke wies auf die Notwendigkeit einer Reform der Datenschutzgesetze hin; die bestehenden Datenschutzgesetzes seien 6 bis 7 Jahre alt. Dies führe dazu, daß den bei Gesetzerlaß noch nicht absehbaren Entwicklungen nur noch mit mühseligen Zusatzinterpretationen Rechnung getragen werden könne. Er verwies auf den von der SPD-Bundestagsfraktion eingebrachten Novellierungsentwurf zum BDSG und darin enthaltene Vorschläge zur Verbesserung des Datenschutzes, wie z.B. verbesserte Auskunftsrechte und -möglichkeiten, kostenlose Auskunft, besser formulierte Zweckbindung und ein ausdrückliches Verbot der Schaffung von Persönlichkeitsprofilen sowie Einschränkungen bei der Verarbeitung von Daten in bestehenden Arbeitsverhältnissen. Auch die Datenschutz-Aufsicht im privatwirtschaftlichen Bereich müsse sachlich verbessert werden.

   Angesichts der Untätigkeit des Bundes müßten die Länder entsprechende datenschutzrechtliche Initiativen erwägen. Nordrhein-Westfalen habe zum Beispiel vor einigen Wochen einen eigenen Entwurf zur Reformierung des Datenschutzrechts auf Länderebene vorgelegt. Der dortige Entwurf werde auch Anlaß für Diskussionen im Bayerischen Landtag sein.

   Im Polizeibereich vertrat der Mitberichterstatter die Ansicht, auch wenn zwei Beanstandungen ausgesprochen worden seien, dürfe nicht verkannt werden, daß die Ermittlungsergebnisse von der Zahl der jeweiligen Ermittler abhänge. Zwischen der Kontrolle einerseits und der Entdeckung von Verstößen andererseits bestehe ein unmittelbarer Zusammenhang. Die Aktenbereinigung durch das Bayerische Landeskriminialamt hob er als vorbildlich hervor, verwies aber auf seine kritische schriftliche Anfrage zur Datenbereinigung beim PP München.

   Im Anschluß erörterte der Ausschuß datenschutzrechtliche Probleme im Bereich der kommunalen Planung und der kommunalen Statistik, die Stellung des kommunalen Datenschutzbeauftragten sowie die Aussagen des

Bundesverfassungsgerichts im Volkszählungsurteil zur Notwendigkeit einer Vollzählung.

2. Im Bayerischen Senat wurde nach der Vorstellung des Tätigkeitsberichts durch den Landesbeauftragten für den Datenschutz im Rechts- und Verfassungsausschuß datenschutzrechtliche Probleme im Bereich der neuen Medien, insbesondere bei der Umsetzung der Datenschutzregelung im Bildschirmtext-Staatsvertrag erörtert. Eine lebhafte Diskussion entwickelte sich zur Frage der Zulässigkeit der Telefondatenerfassung im staatlichen Bereich. Die Mitglieder des Ausschusses begrüßten die Anregung des Datenschutzbeauftragten bei der Vorlage von Gesetzentwürfen nicht nur die Frage nach Kosten und Alternativen der vorgesehenen Regelungen anzusprechen, sondern auch kurz auf die Auswirkungen des Gesetzesvorhabens auf Erhebung und Nutzung personenbezogener Daten einzugehen. Angesprochen wurde auch die Frage, ob der Straf- und Zivilprozeß in der heutigen Form dem Persönlichkeitsschutz eigentlich noch gerecht werde. Aus dem Bereich des Meldewesens wurden die Fragen der Sperrung von Auskünften aus dem Melderegister, die Übermittlung von Wähleranschriften an politische Parteien sowie die Folgen der Automatisierung des Meldewesens erörtert.

25. Arbeitsbedingungen der Geschäftsstelle

Die Personalkapazität der Geschäftsstelle reicht für die anfallende Arbeit bei weitem nicht aus. In meinem 6. Tätigkeitsbericht habe ich hierzu unter derselben Überschrift nähere Darlegungen gemacht. Sie enden mit der Hoffnung auf Unterstützung von Landtag und Staatsregierung bei der Zurverfügungstellung von drei weiteren Planstellen. Diese Hoffnung hat sich nur teilweise erfüllt. Nach den diesmal ausschließlich von der Staatskanzlei geführten Verhandlungen über den Personalhaushalt mit dem Bayerischen Staatsministerium der Finanzen hat der Leiter der Staatskanzlei in einem Schreiben an den Staatsminister der Finanzen wenigstens um die Umsetzung von drei entsprechenden Stellen aus anderen Einzelplänen zur Geschäftsstelle des Landesbeauftragten für den Datenschutz gebeten. Im Laufe der weiteren Verhandlungen mußte ich mich stattdessen mit drei Abordnungsstellen für Haushaltsjahre 1985/86 begnügen. Bei Abordnungsstellen darf das abgebende Ressort die entsprechenden Stellen während der Abordnungszeit des Beamten nicht besetzen. Ich wies daher auf die Schwierigkeiten hin, auf der Basis von Abordnungsstellen Personal für die Geschäftsstelle zu erhalten. Auch der Vorsitzende des Beirats beim Landesbeauftragten für den Datenschutz hat sich mehrfach nachdrücklich für eine Personalaufstockung eingesetzt.

Im Haushalt 1985/86 sind demnach bei der Geschäftsstelle des Landesbeauftragten für den Datenschutz drei Abordnungsstellen vorgesehen. Wie befürchtet war es bisher nicht möglich, auch nur eine dieser Abordnungsstellen zu besetzen. Der Landesbeauftragte für den Datenschutz wird deshalb für den Doppelhaushalt 1987/88, dessen Entwurf im Jahre 1986 zu beraten ist, erneut Anstrengungen unternehmen, eine Personalmehrung zu erreichen, die im übrigen auch durch die Aufgabenmehrung im Bereich der Neuen Medien zwingend erforderlich ist.

26. Konferenz der Datenschutzbeauftragten

Die Datenschutzbeauftragten der Länder und des Bundes und die Datenschutzkommission Rheinland-Pfalz haben im Berichtsjahr in 3 Tagungen gemeinsam interessierende Fragen erörtert. Beispielhaft sei genannt die Erarbeitung einer gemeinsamen Entschließung zu den Auswirkungen des Volkszählungsurteils (abgedruckt als Anhang Nr. 3 zum 6. Tätigkeitsbericht), die Erörterung der Auswirkungen des Volkszählungsurteils auf Mikrozensus, Volkszählung, Hochschulstatistik und andere Statistiken, Überlegungen zur gesetzlichen Regelung des Datenschutzes bei der Kabelkommunikation (Erklärung zur Kabelkommunikation siehe Anhang 5 zum 6. Tätigkeitsbericht), zu Datenschutz bei Bildschirmtext, zum Telefonfernwirksystem der Post (Erklärung der Datenschutzbeauftragten zu TEMEX in Anhang 5 a im 6. Tätigkeitsbericht), zur Mitteilung in Zivilsachen (MiZi) und zum Fahrzeugregister (ZEVIS).

Anhang Nr. 1

Gemeinsames Kommunique vom 5. Oktober 1984 über das Bankauskunftsverfahren

Einigkeit über die Erteilung von Bankauskünften haben die Kreditwirtschaft, die für den Datenschutz im privaten Bereich zuständigen Behörden (Düsseldorfer Kreis) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erzielt. Ziel der Verhandlungen war es, die datenschutzrechtlichen Voraussetzungen und Grenzen des Bankauskunftsverfahrens zu präzisieren, die Kunden über Inhalt und Zweck dieses Verfahrens umfassend zu unterrichten und sie auf ihre Rechte hinzuweisen. In die Gespräche ist auch das Schufa-Verfahren einbezogen worden.

I. In der Diskussion haben sich die Beteiligten von dem Grundsatz leiten lassen, daß dem Vertrauensverhältnis zwischen Kunden und Kreditinstitut (Bankgeheimnis) – unverändert – wesentliche Bedeutung zukommt. Deshalb dürfen Bankauskünfte nur erteilt werden, sofern dies dem Willen des Kunden entspricht. Darüber hinaus können Kreditinstitute aufgrund gesetzlicher Bestimmungen verpflichtet sein, Auskünfte zu erteilen (z.B. im Strafverfahren, Steuerverfahren). Für das Bankauskunftsverfahren gelten nunmehr folgende Anforderungen:

1. Das Kreditinstitut ist berechtigt, über Geschäftskunden (juristische Personen und Kaufleute) Bankauskünfte zu erteilen, sofern ihm keine anderslautende Weisung des Kunden vorliegt.

2. Bankauskünfte über Privatkunden erteilt das Kreditinstitut nur dann, wenn diese allgemein oder im Einzelfall ausdrücklich zugestimmt haben.

3. Bankauskünfte sind allgemein gehaltene Feststellungen und Bemerkungen über die wirtschaftlichen Verhältnisse des Kunden, seine Kreditwürdigkeit und Zahlungsfähigkeit; betragsmäßige Angaben über Kontostände, Sparguthaben, Depot- oder sonstige dem Kreditinstitut anvertraute Vermögenswerte sowie Kreditinanspruchnahmen werden nicht gemacht.

4. Bankauskünfte erhalten nur eigene Kunden sowie andere Kreditinstitute für deren eigene Zwecke und die ihrer Kunden; sie werden nur dann erteilt, wenn der Anfragende ein berechtigtes Interesse an der gewünschten Auskunft glaubhaft darlegt.

II. Für die Durchführung des Bankauskunftsverfahrens wird ergänzend auf folgendes hingewiesen:

1. Die Auskunftsverweigerung wegen fehlender Einwilligung ist so zu formulieren, daß sie nicht als negative Auskunft verstanden werden kann. Liegt bei Privatkunden eine Einwilligung nicht vor oder hat bei Geschäftskunden der Kunde die Erteilung einer Auskunft untersagt oder hat die angefragte Stelle keinen Einblick in die wirtschaftlichen Verhältnisse des Kunden, ist dies in der Antwort deutlich zum Ausdruck zu bringen.

2. Die Auskunft darf sich nur auf die wirtschaftlichen Verhältnisse des Kunden und sein Verhalten im Geschäftsleben beziehen.

3. Bankauskünfte werden nur aufgrund von Erkenntnissen erteilt, die der auskunftgebenden Stelle vorliegen. Es werden keine Recherchen (etwa mit Hilfe von Wirtschaftsauskunfteien) angestellt.

4. Hat das Kreditinstitut eine von Anfang an unrichtige Auskunft erteilt, so ist es zur Richtigstellung gegenüber dem Auskunftsempfänger verpflichtet.

5. Der Kunde, der eine Auskunft erhält, ist ausdrücklich darauf hinzuweisen, daß er empfangene Informationen nur für den angegebenen Zweck verwenden und nicht an Dritte weitergeben darf.

6. Mündlich erteilte Bankauskünfte werden dokumentiert und sollen in der Regel schriftlich bestätigt werden.

7. Auf Verlangen des Betroffenen hat das Kreditinstitut den Inhalt einer erteilten Auskunft mitzuteilen.

8. Wirtschaftsauskunfteien erhalten keine Bankauskünfte.

III. Schufa-Verfahren

1. Es besteht Einvernehmen, daß der Kunde auch über das Schufa-Verfahren ausführlicher und deutlicher unterrichtet werden soll. Die Schufa-Klausel wurde noch nicht abschließend erörtert, weil zunächst der Ausgang eines beim Bundesgerichtshof schwebenden Rechtsstreits abgewartet werden soll, der über die Wirksamkeit der Schufa-Klausel geführt wird.

2. Die Datenschutzbehörden weisen darauf hin, daß eine Datenübermittlung an die Schufa ein Geschäft mit Kreditrisiko voraussetzt. Sie folgern hieraus, daß für die Eröffnung eines Girokontos, das nur auf Guthabenbasis geführt werden soll, die Unterzeichnung der Schufa-Klausel nicht verlangt werden darf. Sie fordern deshalb die Kreditwirtschaft auf, die Errichtung von Girokonten, die nur auf Guthabenbasis geführt werden sollen, auch ohne Schufa-Klausel zu ermöglichen.

Die Vertreter der Kreditwirtschaft weisen demgegenüber darauf hin, daß ein ausschließlich auf Guthabenbasis zu haltendes Konto von seiten des Kreditinstituts eine spezielle Beobachtung erfordert, was die organisatorischen Möglichkeiten eines automatisierten Massengeschäfts überschreiten kann. Außerdem machen sie darauf aufmerksam, daß der Kunde auf verschiedene moderne Formen des Zahlungsverkehrs (ec-Scheck,GAA-Karte) verzichten müßte.

Anmerkung zum Schufa-Verfahren:

Die Entscheidung des Bundesgerichtshofs ist inzwischen ergangen (vgl. oben, Nr. 20 des Berichts).

Anhang Nr. 2

Wartung und Fernwartung

Im folgenden wird eine im Arbeitskreis „Technische und organisatorische Datenschutzfragen" ausgearbeitete Orientierungshilfe wiedergegeben, an deren Erstellung Bayern wesentlich mitwirkte. Bei der Wartung und bei Einsatz der Fernwartung von DV-Systemen durch den Hersteller hat der Kunde (Betreiber des Rechenzentrums) die Einhaltung folgender Datensicherungsmaßnahmen zu beachten:

1. Maßnahmen zur Zugangskontrolle

1.1 Zugangskontrolle der Wartung vor Ort

Das Personal, das die Wartungsarbeiten an der DV-Anlage durchführt, hat sich denselben Legitimationsprüfungen zu unterwerfen, wie das eigene Personal, das an der DV-Anlage arbeitet (Ausweiskarte, persönliches Kennwort). Bei der Fernwartung muß sich der Wartungstechniker mit Benutzernummer und persönlichem Kennwort identifizieren. Außerdem hat bei der Fernwartung der Verbindungsaufbau stets vom Kunden aus zu erfolgen.

1.2 Sicherstellung, daß vom Maschinenbediener nur die Wartungszentrale angerufen werden kann.

Bei Benutzung des Datex-L-Netzes bietet die Deutsche Bundespost eine Einrichtung für Direktruf (Kosten mtl. DM 5.-) an, mit der ausschließlich eine bestimmte Fernsprechnummer, die in den Rechner einprogrammiert wurde, angewählt werden kann. Im herkömmlichen Fernsprechnetz kann der Spezial-Fernsprechapparat Typ 756DD (Kosten mtl. DM 5.80) nach Eingabe der Rufnummer nur zu dieser Rufnummer die Verbindung herstellen. Die Rufnummerneingabe läßt sich durch einen Schlüssel sichern. Auf diese Weise wird verhindert, daß ein unbefugter Teilnehmer Zugriff auf das System erhält, wenn er einen Komplicen am Rechner hat.

1.3 Kontrolle des Fernwartungsvorgangs

Der Fernwartungsvorgang muß vom Betreiber der DV-Anlage jederzeit abgebrochen werden können.

2. Organisation der Abgangskontrolle

2.1 Prüfung der aus dem Rechenzentrumsbereich hinausgehenden Datenträger

Bevor Datenträger mit personenbezogenen Daten aus dem Rechenzentrumsbereich zu Wartungszwecken oder zur Fehleranalyse hinausgegeben werden, ist eine besondere Erlaubnis durch autorisiertes Rechenzentrumspersonal einzuholen. Mit Rechenzentrumspersonal ist das für die Bedienung der Datenverarbei tungsanlage vom Betreiber der Anlage eingesetzte und mit entsprechender Befugnis versehene Personal gemeint. Auf einem Begleitschein, der zugleich als Beleg für die Abgangs- und Rücklaufkontrolle verwendet wird, sind die Art der Daten und des Datenträgers zu vermerken.

2.2 Behandlung wartungseigener Datenträger

Es ist sicherzustellen, daß das Wartungspersonal nicht mit den eigenen mitgebrachten Datenträgern (Magnetbänder und Magnetplatten) die Wartung durchführt, sondern ausschließlich mit Duplikaten arbeitet, die im Rechenzentrum erstellt werden und dort für Kontrollzwecke (mindestens 1 Jahr) aufzubewahren sind. Werden Test- und Service-Programme des Herstellers auf der Anlage gespeichert, sind diese unter einer besonderen Kennung abzulegen.

3. Maßnahme zur Speicherkontrolle

Der Betreiber des Rechenzentrums muß Dateien und Programme durch Paßworte schützen, soweit diese bei der Wartung physisch im Zugriff bleiben.

3.1 Vergabe und Verwaltung der Paßwörter

Die Vergabe und Verwaltung der Paßwörter muß ausschließlich den dazu autorisierten Personen des Rechenzentrumspersonals obliegen.

3.2 Wartung der heißen Anlage

Müssen Wartungs- und Diagnosearbeiten an der Herstellersoftware im laufenden Betrieb durchgeführt werden, so dürfen diese nur unter ständiger Kontrolle eines sachkundigen Mitarbeiters des Rechenzentrums erfolgen. (Nach den VDE-Schutzbestimmungen dürfen auch Arbeiten an Starkstromgeräten nie ohne Anwesenheit weiterer Personen ausgeführt werden).

3.3 Zugriff auf personenbezogene Daten

Ist für Wartungszwecke ein Zugriff auf personenbezogene Daten erforderlich, kann das nur nach ausdrücklicher Genehmigung durch die verantwortliche Stelle erfolgen. Der Zugriff auf personenbezogene Daten sollte allerdings nur den Ausnahmefall darstellen. Nicht benötigte Dateien sind aus dem direkten Zugriff zu entfernen. U.U. sind ganze Laufwerke abzuschalten.

3.4 Einspielen neuer Releases ins Betriebssystem und in systemnahe Software

Das Einspielen von Änderungen ins Betriebssystem und in system nahe Software unmittelbar innerhalb der Fernwartung ist abzulehnen. Solche Änderungen sind ausschließlich im Rechenzentrum durchzuführen. Im Zuge der Fernwartung notwendige Änderungen sind ausschließlich in einer besonderen Datei im System des Rechenzentrums einzuspeichern. Die Durchführung der Änderungen ist erst nach Freigabe durch autorisiertes Rechenzentrumspersonal vorzunehmen.

Bei der Wartung vor Ort hat die Änderung des Betriebssystems und der systemnahen Software nur durch den Systemverantwortlichen bzw. im Beisein einer sachkundigen Person des Betreibers der DV-Anlage zu erfolgen.

4. Maßnahmen zur Zugriffskontrolle

4.1 Offenbarung von Kundenpaßwörtern

Für den Fall, daß in einem Wartungsvorgang ein Zugriff auf Dateien mit personenbezogenen Daten oder direkt auf die Paßwortdatei notwendig ist, sind nach Abschluß der Wartungsarbeiten die der Wartung offenbarten Paßwörter unverzüglich zu ändern.

4.2 Überprüfen der Wartungsprotokolle

Die Aktivitäten eines Wartungsvorgangs, die in einer Protokolldatei festzuhalten sind, sind zu überprüfen und mindestens ein Jahr aufzubewahren. Die Verpflichtung des Systemverantwortlichen den Wartungsvorgang am Bildschirm zu verfolgen und die Verbindung in kritischen Fällen zu unterbrechen bleibt davon unberührt.

5. Maßnahmen zur Auftragskontrolle

5.1 Wartungsvertrag

Im Wartungsvertrag sind klare Regelungen hinsichtlich der Abgrenzung der Kompetenzen und Pflichten zwischen Wartungs- und Rechenzentrumspersonal zu treffen. Art und Umfang der Wartung (Hard- und Software) sind schriftlich festzulegen.

5.2 Sicherheitsanforderungen an das Wartungspersonal

Der Hersteller muß vertraglich versichern, daß das Wartungs personal sicherheitsüberprüft und auf das Datengeheimnis verpflichtet ist.

5.3 Weitergabe der übertragenen Daten

Eine abermalige Weitergabe der Daten, die der Wartung übergeben oder bei der Fernwartung übertragen wurden, ist vertraglich zu untersagen bzw. streng zu reglementieren. Ist zur Fehlerbehebung eine Weitergabe der übergebenen Kundendaten an Tochter- oder das Mutterunternehmen im Ausland notwendig, müssen die Sicherheitsmaßnahmen wie im Inland eingehalten werden.

5.4 Behandlung der übergebenen bzw. übertragenen Daten nach Aufgabenerledigung

Soweit es sich nicht um reine Hardwaredaten handelt, ist vertraglich zu vereinbaren, daß übergebene bzw. übertragene Daten im Wartungszentrum nur temporär aufbewahrt bzw. gespeichert werden dürfen und nach Erledigung sofort zu vernichten bzw. zu löschen sind.

5.5 Vereinbarung über den Einsatz der Fernwartung

Hinsichtlich der Fernwartung wird empfohlen einen separaten schriftlichen Vertrag abzuschließen, in dem die Einhaltung besonderer Datensicherungsmaßnahmen, die festzulegen sind, vereinbart wird.

6. Maßnahmen zur Transportkontrolle

6.1 Transportweg

Der Transportweg für Datenträger (Magnetbandrollen, Listen usw.) und die am Transportweg beteiligten Personen sind festzulegen. Darüber hinaus empfiehlt es sich eine Sicherheitsanalyse durchzuführen.

6.2 Materielle Datensicherungsmaßnahmen

Es ist zu prüfen, ob beim Versand von Datenträgern für Wartungszwecke die Versandart angemessen und ausreichend ist. Darüber hinaus ist eine Vollständigkeitsprüfung vorzusehen. Beim Transport von Datenträgern sind grundsätzlich Begleitpapiere zu benützen.

7. Maßnahmen zur Organisationskontrolle

7.1 Dokumentation

Der Betreiber des Rechenzentrums ist gehalten, das Wartungs- bzw. Fernwartungskonzept schriftlich zu dokumentieren (Kontrolle der technischen und organisatorischen Maßnahmen zum Datenschutz).

Anhang Nr. 3

Orientierungshilfe für Sicherungsmaßnahmen bei der Mikroverfilmung von Schriftgut

Diese Orientierungshilfe wurde im Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 1984 beraten; sie wurde im Juni 1985 an den Stand der Technik angepaßt und fortgeschrieben.

Vorbemerkung:

Mikroverfilmte Bestände lassen sich grundsätzlich besser vor unberechtigten Zugriff schützen als herkömmlich organisierte Archivbestände in Papierform. Die Anwendung von Datensicherungsmaßnahmen auf Mikrofilme und Mikrofiche ist wirksamer. Außerdem existieren eine Reihe technischer Datensicherungsmaßnahmen, die auf das Medium „Papier" in analoger Weise nicht übertragbar sind.

Folgende Sicherungsmaßnahmen sind nur bei Mikrofilm/fiche-Archiven anwendbar:

- Der Mikrofilm/fiche-Bestand kann feuer- und zugriffssicher auf bewahrt werden.
- Eine falsche Einordnung gelesener Dokumente ist nicht möglich.
- Die Vollständigkeitskontrolle läßt sich wesentlich leichter durchführen.
- Bestimmte Filme (C-Filme) können nicht dupliziert werden.
- Leichtere Trennung der Zugriffsberechtigung für Lesen und Kopieren (interessant für Archive und Vorgänge, bei denen keine Kopien angefertigt werden dürfen) durch technische Geräte (Auf stellen von Lesegeräten, bei denen die Rückvergrößerung und das Erstellen von Kopien nicht möglich ist).
- Die Zugriffsberechtigung auf bestimmte Vorgänge läßt sich über „geblipte Filme" steuern, so daß ein Zugriff auf die Seiten nur mit einem bestimmten Kennwort möglich ist.

Beim Vorgang der Verfilmung treten im Prinzip dieselben Probleme wie bei der Papierverarbeitung auf.

Arbeitsschritte bei der Mikroverfilmung sind:

- Die Vorbereitung des Schriftgutes (ggf. der Transport zur verfilmenden Stelle)
- Die eigentliche Verfilmung
- Entwicklung des Films und die Filmkontrolle
- Die Prüfung des Verfilmungsergebnisses
- Die Vernichtung des verfilmten Schriftgutes
- Die Verwaltung des Mikrofilm/fiche-Bestandes

Grundsätzlich unterscheidet man zwischen
der Passivverfilmung (Altaktenbestände) und
der Aktivverfilmung (aktuelle Vorgänge).

Bildträger sind
der Rollfilm
das Jacket und
der Mikrofiche.

Bei den nachfolgend aufgeführten Sicherungsmaßnahmen ist eine Anwendung stets unter den Grundsatz der Angemessenheit zu prüfen.

1. **Vorbereitung des Schriftgutes**

Aufbereitung des Schriftgutes zur Verfilmung:

- Entfernung der Metallteile (Heft-, Büroklammern u.ä.)
- Glätten, chronologisches Einordnen, Sortieren, Reduzieren (z.B. Entfernen von Duplikaten)
- Durchnumerieren der Vorgänge (bei besonders sensiblen Unterlagen)
- Abgabe zur Verfilmungsstelle
- Transport zum Verfilmer

Risiken:

- Unvollständigkeit des Schriftgutes
  Zusätzlich bei der Verfilmung außer Haus:
  – unzulässige Offenbarung
  – Transportrisiken (Verlust, Diebstahl)

Sicherungsmaßnahmen:

- Stichprobenhafte Prüfung des Schriftgutes
- Zählung der aufbereiteten Vorgänge (Schriftstücke)
- Aufbereitung durch eigenes Personal
- sorgfältige Auswahl des Auftragnehmers nach Sicherheitsstandard (eventl. Ortsferne)
- Vertragsgestaltung (Verpflichtung zur Verschwiegenheit, Auflagen für Transport und Aufbewahrung)
- Transportsicherungen
- Transport durch eigenes Personal

2 **Verfilmung:**

Beachtung der geltenden DIN-Normen

Verwendung der Mikrofilm-Bildzeichen

Einzelblattverfilmung:
- seitenweise
- blattweise Vorder- und Rückseite zugleich
- Duplikatrollfilmerstellung in einem Arbeitsgang

Anlage der Verfilmungskartei mit folgenden Informationen:
- Aktenplannummer
- Sachgebiet
- Filmrollen-, Zählerstandsnummer
- Fallidentifizierung

Risiken:

Unvollständige Schriftgutverfilmung

unbefugte Offenbarung von Inhalten

unberechtigte Nutzung des verfilmten Schriftgutes bis zur Vernichtung
Zusätzlich bei Verfilmung außer Haus:
- Transportrisiken
- unberechtigte Nutzung des verfilmten Schriftgutes beim Auftragnehmer

Sicherungsmaßnahmen:

Kennzeichnen der zu verfilmenden Unterlagen durch automatisches Numerieren, Zählwerkkontrollen und Bearbeitungsstempel

Einblendung von Bildmarkennummern (Blips) zur späteren Zugriffskontrolle

Anmietung einer Verfilmungsanlage („mobilen Kamera"), um eine Außerhausverfilmung zu vermeiden und ggf. Verfilmung durch eigenes Personal

Verschluß des verfilmten Materials

Kontrolle der verbrauchten Rollfilme

Speicherkontrolle (Verfilmer, Datum)
Bei Außerhausverfilmung:
- Verfilmung unter Aufsicht eigenen Personals
- sorgfältige Auswahl des Auftragnehmers (an der Sache uninteressiert) nach Sicherheitsstandards
- Eigentransport
- Transport in verschlossenen Behältnissen
- Vollständigkeitskontrolle (soweit möglich)
- ergänzende Absicherungen durch vertragliche Regelungen

3 **Entwickeln des Films und Filmkontrolle:**

Entwickeln der belichteten Rollfilme

Duplizieren des Filmes

Risiken:

Transportrisiken

unberechtigte Anfertigung von Filmkopien

Sicherungsmaßnahmen:

Eigenentwicklung

- Abzählen des Materials
- Vernichtung der Testfilme
  Zusätzlich bei Entwicklung außer Haus:
  - Transport per Kurier
  - höherwertige Versandart auf dem Postweg
  - Begleitpapiere (z.B. Anzahl der Filme, Längenangaben 35/65 m)
  - sorgfältige Auswahl des Auftragnehmers
  - ergänzende, vertragliche Absicherungen
  - Verfilmung und Entwicklung in einem Arbeitsgang

4. **Prüfung des Verfilmungsergebnisses:**

- Lesbarkeit des Filmes
- Wiedergabefähigkeit (Rückvergrößerung)
- Verwendung der Bildzeichen
- Vollständigkeit der Blattnummern innerhalb eines Falles (stichprobenweise; bei Vorgabe numerierter Vorgänge)
- Anlegen der Verfilmungskartei mit folgenden Informationen:
  - Blip-Nummer
  - Hinweis auf Verbleib von Originalunterlagen
  - Prüfvermerk

Risiken:

- unvollständige Verfilmung
- Verlust der Verfilmungskartei

Sicherungsmaßnahmen:

- Nachverfilmung fehlender Vorgänge/Blätter (Prüfung des Filmes)
- Zugangssicherung
- Zugriffssicherung
- Verfilmung der Verfilmungskartei in gewissen Zeitabständen (gleichzeitig oder später)

5. **Vernichtung des verfilmten Schriftgutes:**

Risiken:

- Unvollständige und schlechte Entsorgung

Sicherungsmaßnahmen:

- Vernichtung im eigenen Reißwolf
- Aufbewahrung im abschließbaren Zwischenlager
- Transport und Vernichtung unter Aufsicht, auch bei Auftragsvergabe
- sorgfältige Auswahl eines Auftragnehmers nach Sicherheitsstandard

6. **Verwaltung des Filmguts:**

- Rollfilmverwaltung
- Jacketverwaltung
- Mikroficheverwaltung
- Erzeugung von Sicherungsbeständen

- Aufbewahrung der Sicherungsbestände
- Löschen und Sperren von verfilmten Einzelfällen

Risiken:

- Bestandsverlust
- unberechtigte Vervielfältigung von Rollfilmen, Filmjackets und Mikrofiches
- unberechtigter Zugriff auf Sicherungsbestände

Sicherungsmaßnahmen:

- Aufbewahrung unter Verschluß
- Aufbewahrung in Schuppenordnern (leichtere Vollzähligkeitsprüfung)
- Kontrolle der Ausgabe und Rückgabe des Filmguts
- Lesen unter Aufsicht
- nur Lesegeräte zur Verfügung stellen
- Duplizieren nur nach Auftrag
- Rückgabe von Fehlverfilmungen
- Kontrolle des Dupliziervorgangs (Zählwerk am Gerät)
- Protokoll über Dupliziervorgang (evt. 4-Augen-Prinzip)
- Arbeitsexemplar nicht duplizierbar durch Verwendung entsprechenden Filmmaterials
- Trennung von Sicherungskopien und Arbeitsexemplaren des Filmgutes
- Sicherungskopien räumlich oder örtlich getrennt zugriffssicher lagern
- Vernichtung der entsprechenden Verfilmungskarteikarte beim Löschen eines Falles
- Hinweis auf Verwendungssperre in der Verfilmungskarteikarte anbringen
- Zählen der Rückvergrößerungskopien durch Abgleich mit Aufträgen